

Dominion KX III

User Guide

Release 3.5.0

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior written consent of Raritan, Inc.

© Copyright 2018 Raritan, Inc. All third-party software and hardware mentioned in this document are registered trademarks or trademarks of and are the property of their respective holders.

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

この装置は、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。

VCCI-A

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.

If a power cable is included with this product, it must be used exclusively for this product.



Welcome

Contents

Dominion KX III Release 3.5.0 User Guide

What's New in KX III Release 3.5.0

- Test your RADIUS connection: *Implementing RADIUS Remote Authentication* (on page 80)
- PC Share Timeout setting: *Encryption and Share* (on page 193)
- *Enabling TLS Protocols* (on page 197)
- Support for multiple Subject Alternative Names (SAN) in certificates: *SSL Certificates* (see "*SSL and TLS Certificates*" on page 200)
- Show or hide client toolbar and status bar: *Client Launch Settings* (on page 281)
- HTML KVM Client updates:
 - *HTML KVM Client (HKC) Help* (on page 305)
 - Support for French Keyboard: *Keyboard Layout* (on page 312)
 - *Import and Export Macros* (on page 316)
 - *Send Text to Target* (on page 317)
 - Macro for Print Screen: *Send Macro* (on page 313)
 - *Virtual Media Menu* (on page 329)
 - *Audio Menu* (on page 332)
 - *Power Control Menu* (on page 334)
 - Support for Dual Video Targets on Chrome and Firefox

Welcome **iii**

Chapter 1 Introduction **1**

Overview	1
Package Contents	2
KX III Device Photos and Features	2
Hardware	2
Software	3
Dominion KX3-832	5
Dominion KX3-864	6
Supported Number of Ports and Remote Users per Model	7
KX III Remote/Local Console Interfaces and User Station	8
KX III KVM Client Applications	8
KX III Online Help	9

Chapter 2 Get Started Using KX III **10**

Install and Configure KX III	10
Factory Default Login Information	10
Allow Pop-Ups	10
Security Warnings and Validation Messages	11
Java Validation and Access Warning	11
Additional Security Warnings	12
Installing a Certificate	12
Example 1: Import the Certificate into the Browser	12
Example 2: Add the KX III to Trusted Sites and Import the Certificate	14
Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional)	16
Logging In to KX III	18

Chapter 3 KX III Interface and Navigation **19**

Overview	19
KX III Remote Console Interface	20
Port Access Page (Remote Console Display)	21
Port Action Menu	24
DKX3-808 Fast Switching	27
Left Panel	28
KX III Local Console Interface	30
Overview	30
KX III Installation and Configuration	30
Rack Mounting	31
Factory Default Login Information	32
Step 1: Configuring Network Firewall Settings	32

Step 2: Configuring KVM Target Servers	33
Step 3: Connecting the Equipment.....	36
Step 4: Configuring the KX III.....	38
Step 5: Launching the KX III Remote Console	48
Step 6: Configuring the Keyboard Language (Optional)	50
Step 7: Create and Install an SSL Certificate	51
Rack PDU (Power Strip) Outlet Control	51
Overview.....	51
Turning Outlets On/Off and Cycling Power	52
USB Profiles	54
Overview.....	54
CIM Compatibility	54
Available USB Profiles	55
Selecting Profiles for a KVM Port.....	61
User Management.....	61
User Groups.....	61
Users	70
Authentication Settings.....	74
Changing a Password.....	86
Device Management.....	87
Network Settings.....	87
View and Edit LAN Interface Settings	93
Reset Network Settings to Factory Defaults	95
Configuring Ports	96
Device Services.....	143
Power Supply Setup	176
Connect and Disconnect Scripts	178
Port Group Management	183
Changing the Default GUI Language Setting.....	186
Security Management.....	187
Security Settings	187
Configuring IP Access Control.....	198
SSL and TLS Certificates	200
Security Banner.....	203
Maintenance	205
Audit Log.....	205
Device Information	206
Creating a KX III Backup and Restore File.....	207
Applying KX III Appliance Setting to a KX III Using a Backup/Restore File.....	210
USB Profile Management	211
Upgrading CIMs.....	212
Upgrading the KX III Firmware	213
Upgrade History	214
Rebooting the KX III.....	214
Stopping CC-SG Management.....	216

Diagnostics	217
Network Interface Page	217
Network Statistics Page.....	217
Ping Host Page	218
Trace Route to Host Page	219
Device Diagnostics	220
KX III Local Console - Administration Functions.....	221
Security and Authentication.....	221
Configuring KX III Local Port Settings from the Local Console.....	222
Command Line Interface (CLI)	226
Overview.....	226
Accessing the KX III Using CLI.....	226
SSH Connection to the KX III.....	226
Logging In	227
Navigating the CLI	227
Initial Configuration Using CLI	229
CLI Prompts.....	230
CLI Commands	230
Administering the KX III Console Server Configuration Commands.....	231
Configuring Network.....	231
Dual Video Port Groups	233
Recommendations for Dual Port Video.....	234
Dual Video Port Group Supported Mouse Modes	234
CIMs Required for Dual Video Support	235
Dual Port Video Group Usability Notes	235
Permissions and Dual Video Port Group Access.....	236
Example Dual Port Video Group Configuration	237
Dual Port Video Configuration Steps.....	238
Raritan Client Navigation when Using Dual Video Port Groups	241
Direct Port Access and Dual Port Video Groups	242
Dual Port Video Groups Displayed on the Ports Page.....	242

Chapter 4 Virtual Media 243

Overview	243
Prerequisites for Using Virtual Media	244
KX III Virtual Media Prerequisites	244
Remote PC VM Prerequisites	244
Target Server VM Prerequisites	244
CIMs Required for Virtual Media	244
Mounting Local Drives	245
Notes on Mounting Local Drives	245
Supported Tasks Via Virtual Media	245
Supported Virtual Media Types	246
Conditions when Read/Write is Not Available	246

Supported Virtual Media Operating Systems	246
Number of Supported Virtual Media Drives	247
Connecting and Disconnecting from Virtual Media.....	247
Access a Virtual Media Drive on a Client Computer.....	247
Mounting CD-ROM/DVD-ROM/ISO Images	248
Disconnect from Virtual Media Drives	249
Virtual Media in a Windows XP Environment.....	249
Virtual Media in a Linux Environment.....	250
Active System Partitions	250
Mapped Drives	250
Drive Partitions.....	250
Root User Permission Requirement	250
Connect Drive Permissions (Linux)	251
Virtual Media in a Mac Environment	252
Active System Partition.....	252
Drive Partitions.....	252
Connect Drive Permissions (Mac)	253
Virtual Media File Server Setup (File Server ISO Images Only).....	253

Chapter 5 KX III KVM Clients 255

KX III KVM Client Launching	255
Virtual KVM Client (VKC and VKCs) Help	256
Overview.....	256
Recommended Minimum Virtual KVM Client (VKC) Requirements	256
Virtual KVM Client Java Requirements.....	257
Proxy Server Configuration for Use with VKC, VKCS, and AKC	258
Connect to a Target from Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC)	259
Configuring Connection Properties.....	260
Connection Information	264
USB Profiles	265
Keyboard.....	266
Video Properties	270
Mouse Options	274
Tool Options.....	278
View Options	287
Connect to Virtual Media.....	288
Smart Cards.....	289
Digital Audio	291
Power Control Using VKC, VKCS, and AKC.....	300
Version Information - Virtual KVM Client.....	300
Active KVM Client (AKC) Help	301
Overview.....	301
Recommended Minimum Active KVM Client (AKC) Requirements	301

AKC Supported Microsoft .NET Framework	301
AKC Supported Operating Systems	302
AKC Supported Browsers	302
Prerequisites for Using AKC	302
Proxy Server Configuration for Use with VKC, VKCS, and AKC	303
Connect to a Target from Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC)	304
HTML KVM Client (HKC) Help	305
Connection Properties	307
Connection Info	311
USB Profile	312
Input Menu	312
Video Menu	323
View Menu	328
Virtual Media Menu	329
Audio Menu	332
Power Control Menu	334

Chapter 6 Serial Access With Dominion Serial Access Module 335

Connect KX III and DSAM	336
DSAM LED Operation	336
Supported USB Device Combinations	337
View DSAM Serial Ports	338
Configure DSAM Serial Ports	338
Configure Serial Port Keyword List	342
Upgrade DSAM Firmware	342
Supported CLI Commands	344
Command Line Interface Shortcuts	348
Command Line Interface High-Level Commands	348
Connect to DSAM Serial Targets with KX3 GUI	348
Connect to DSAM Serial Target with URL Direct Port Access	349
Connect to DSAM Serial Target via SSH	350
Chapter 7 HTML Serial Console (HSC) Help	351
HSC Functions	352

Chapter 8 Dominion KX III User Station 360

Overview	361
User Station Photo and Features	362
Operating the User Station	362

Chapter 9 Mobile KVM Client (MKC) Help 364

Remotely Access Targets Using a Mobile Device	364
Connect to a Target Using the Mobile KVM Client	365
Touch Mouse Functions	365
Using the MKC Toolbar	366
MKC Toolbar Icons	366
Display Mobile Device Keyboard	368
Display Connection Info	368
Set Keyboard Type	369
Keyboard Languages	369
Manage Mobile Client Keyboard Macros	369
Launch Keyboard Macro	370
Set Mouse Mode	370
Absolute Mouse Mode	371
Intelligent Mouse Mode	371
Standard Mouse Mode	371
Sync Mouse in Intelligent or Standard Mouse Mode	372
Auto-Sense Video Settings	372
Set Video Connection Quality	372
View MKC Help	373

Chapter 10 KX III Remote Console 374

Overview	374
Scanning Ports - Remote Console	375
Scanning Ports Slide Show - Remote Console	376
Target Status Indicators During Port Scanning - Remote Console	377
Using Scan Port Options	378
Scan for Targets	379
Changing a Password	380
Managing Favorites	381
Enable Favorites	381
Access and Display Favorites	382
Discovering Devices on the Local Subnet	382
Discovering Devices on the KX III Subnet	383

Chapter 11 KX III Local Console 385

Overview	385
Accessing a Target Server	385
Local Console Video Resolution Behavior	386
Simultaneous Users	386
Local Port Hot Keys and Connect Keys	386
Return to the Local Console from a Target Device - Default Hot Key	387
Local Port Auto-Sense (Video Refresh) - Default Hot Key	387
Connect Key Examples	387
Special Sun Key Combinations	388
Scanning Ports - Local Console	389
Scanning Port Slide Show - Local Console	390
Target Status Indicators During Port Scanning - Local Console	392
Configure Local Console Scan Settings	392
Scan for Targets - Local Console	393
Local Console Smart Card Access	394
Local Console USB Profile Options	395
KX III Local Console Factory Reset	396
Resetting the KX III Using the Reset Button on the Device	397

Appendix A Connecting a KX III and Cat5 Reach DVI - Provide Extended Local Port Functionality 398

About the Cat5 Reach DVI	398
Connect Cat5 Reach DVI and Cat5 Reach DVI	399

Appendix B Accessing a Paragon II from the KX III 402

Overview	402
Supported Paragon II CIMS and Configurations	403
KX III-to-KX III Paragon CIM Guidelines	405
KX III-to-Paragon II Guidelines	406
Supported Connection Distances Between Paragon II and KX III	408
Connecting the Paragon II to the KX III	408

Appendix C Updating the LDAP Schema 409

Returning User Group Information	409
From LDAP/LDAPS	409
From Microsoft Active Directory	409

Setting the Registry to Permit Write Operations to the Schema	410
Creating a New Attribute	410
Adding Attributes to the Class	411
Updating the Schema Cache	413
Editing rcusergroup Attributes for User Members.....	413

Appendix D Specifications 416

Hardware	416
KX III Dimensions and Physical Specifications	416
KX III Supported Target Server Video Resolutions.....	419
KX III Supported Local Port DVI Resolutions.....	420
Target Server Video Resolution Supported Connection Distances and Refresh Rates	421
Supported Computer Interface Module (CIMs) Specifications	421
Supported Digital Video CIMs for Mac	424
Digital CIM Timing Modes.....	425
Digital CIM Established and Standard Modes	425
DVI Compatibility Mode.....	426
Supported Remote Connections.....	427
Network Speed Settings	427
Dell Chassis Cable Lengths and Video Resolutions.....	428
Smart Card Minimum System Requirements	429
Supported Smart Card Readers	430
Unsupported Smart Card Readers.....	431
Audio Playback and Capture Recommendations and Requirements	432
Number of Supported Audio/Virtual Media and Smartcard Connections.....	434
Certified Modems	434
KX III Supported Keyboard Languages.....	434
Mac Mini BIOS Keystroke Commands.....	435
Using a Windows Keyboard to Access Mac Targets.....	437
TCP and UDP Ports Used	437
Software.....	438
Supported Operating Systems, Browsers and Java Versions	438
Virtual KVM Client (VKC), VKCS, and Active KVM Client (AKC) Requirements	440
Multi-Language Keyboard JRE Requirement.....	441
Events Captured in the Audit Log and Syslog.....	442
BSMI Certification	443

Appendix E Informational Notes 444

Overview	444
Java Runtime Environment (JRE) Notes.....	444
Disable Java Caching and Clear the Java Cache.....	444
Java Not Loading Properly on Mac.....	445

Contents

IPv6 Support Notes	446
Operating System IPv6 Support Notes	446
AKC Download Server Certification Validation IPv6 Support Notes	446
Dual Stack Login Performance Issues	447
CIM Notes	447
Windows 3-Button Mouse on Linux Targets	447
Windows 2000 Composite USB Device Behavior for Virtual Media	448
Target Video Picture Not Centered (Mouse Out of Synch)	449
Powerstrip is not detected	449
Virtual Media Notes	449
Cannot Connect to Drives from Linux Clients	449
Cannot Write To/From a File from a Mac Client	449
Virtual Media via VKC and AKC in a Windows Environment	450
Virtual Media Not Refreshed After Files Added	451
Virtual Media Linux Drive Listed Twice	451
Accessing Virtual Media on a Windows 2000	451
Disconnecting Mac and Linux Virtual Media USB Drives	451
Target BIOS Boot Time with Virtual Media	451
Virtual Media Connection Failures Using High Speed for Virtual Media Connections	452
USB Port and Profile Notes	452
VM-CIMs and DL360 USB Ports	452
Help Choosing USB Profiles	452
Changing a USB Profile when Using a Smart Card Reader	454
Video Mode and Resolution Notes	454
Video Image Appears Dark when Using a Mac	454
Video Shrinks after Adjusting Target Clock	454
Black Stripe/Bar(s) Displayed on the Local Port	455
Sun Composite Synch Video	455
SUSE/VESA Video Modes	455
Keyboard Notes	456
French Keyboard	456
Keyboard Language Preference (Fedora Linux Clients)	457
Macros Not Saving on Linux Targets	458
Mac Keyboard Keys Not Supported for Remote Access	459
Mouse Notes	459
Mouse Pointer Synchronization (Fedora)	459
Single Mouse Mode when Connecting to a Target Under CC-SG Control	459
Mouse Sync Issues in Mac OS 10	459
Audio	460
Audio Playback and Capture Issues	460
Audio in a Linux Environment	460
Audio in a Windows Environment	461
Smart Card Notes	461
Virtual KVM Client (VKC) Smart Card Connections to Fedora Servers	461
CC-SG Notes	461
Virtual KVM Client Version Not Known from CC-SG Proxy Mode	461

Moving Between Ports on a Device	461
Browser Notes	461
Resolving Issues with Firefox Freezing when Using Fedora	461

Appendix F Frequently Asked Questions 462

General FAQs	462
Remote Access	465
Universal Virtual Media	468
Bandwidth and KVM-over-IP Performance	470
IPv6 Networking	474
Servers	476
Blade Servers	476
Installation	478
Local Port - KX IIII	481
Extended Local Port	482
Dual Power Supplies	483
Intelligent Power Distribution Unit (PDU) Control	483
Ethernet and IP Networking	485
Local Port Consolidation, Tiering and Cascading	486
Computer Interface Modules (CIMs)	489
Security	490
Smart Cards and CAC Authentication	492
Manageability	493
Documentation and Support	495
Miscellaneous	496

Index 497

Chapter 1 Introduction

The Dominion KX III is an enterprise-class, secure, KVM-over-IP switch that provides multiple users with remote BIOS-level control of 8 to 64 servers.

KX III comes with standard features such as DVI/HDMI/DisplayPort digital and analog video, audio, virtual media, smart card/CAC, blade server support, and mobile access.

Deploy KX III individually, or with Raritan’s CommandCenter Secure Gateway (CC-SG).

In This Chapter

Overview	1
Package Contents	2
KX III Device Photos and Features	2
KX III Remote/Local Console Interfaces and User Station	8
KX III KVM Client Applications	8
KX III Online Help	9

Overview

The Dominion KX III is an enterprise-class, secure, KVM-over-IP switch that provides multiple users with remote BIOS-level control of 8 to 64 servers.

KX III comes with standard features such as DVI/HDMI/DisplayPort digital and analog video, audio, virtual media, smart card/CAC, blade server support, and mobile access.

Deploy KX III individually, or with Raritan’s CommandCenter Secure Gateway (CC-SG).

Package Contents

Each KX III ships as a fully-configured stand-alone product in a standard 1U (2U for KX3-864) 19" rackmount chassis. Each KX III device ships with the following contents:

- 1 - KX III device
- 1 - KX III Quick Setup Guide
- 1 - Rackmount kit
- 2 - AC power cords
- 1 - Set of 4 rubber feet (for desktop use)
- 1 - Application note
- 1 - Warranty card

KX III Device Photos and Features

Hardware

- Integrated KVM-over-IP remote access
- 1U or 2U rack-mountable (brackets included)
- Dual power supplies with failover; autoswitching power supply with power failure warning
- Support for the following CIMs:
 - For virtual media and Absolute Mouse Synchronization, use one of the following CIMs:
 - D2CIM-VUSB
 - D2CIM-DVUSB
 - D2CIM-DVUSB-DVI
 - D2CIM-DVUSB-HDMI
 - D2CIM-DVUSB-DP
 - Required for PS2 connection:
 - DCIM-PS2
- DVI monitor support from the DVI local port
 - VGA support via a DVI to VGA converter
 - DVI support via a standard DVI cable

- Remote access and power management from an iPhone® or iPad®
- Support for tiering in which a base KX III device is used to access multiple other tiered devices
- Multiple user capacity (1/2/4/8 remote users; 1 local user)
- UTP (Cat5/5e/6) server cabling
- Dual Ethernet ports (10/100/1000 LAN) with failover or isolation mode support
- Field upgradable
- Local USB User port for in-rack access
 - USB Keyboard/mouse ports, or connect to a cellular modem
 - One front and three back panel USB ports for supported USB devices
 - Fully concurrent local and remote user access
 - Local graphical user interface (GUI) for administration
- Serial port to connect to an external telephone modem
- Centralized access security
- Integrated power control
- LED indicators for dual power status, network activity, and remote user status
- Hardware Reset button

Software

- Virtual media support in Windows®, Mac® and Linux® environments*
- Absolute Mouse Synchronization*

**Note: Virtual media and Absolute Mouse Synchronization require use of a D2CIM-VUSB, D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI or D2CIM-DVUSB-DP CIM.*

- Support for digital audio over USB
- Port scanning and thumbnail view of up to 32 targets within a configurable scan set
- Web-based access and management
- Intuitive graphical user interface (GUI)
- Support for dual port video output
- 256-bit encryption of complete KVM signal, including video and virtual media
- LDAP, Active Directory®, RADIUS, or internal authentication and authorization
- DHCP or fixed IP addressing
- Smart card/CAC authentication
- SNMP, SNMPv3, SMTP, and Syslog management
- IPv4 and IPv6 support
- Power control associated directly with servers to prevent mistakes
- Integration with Raritan's CommandCenter Secure Gateway (CC-SG) management unit
- CC Unmanage feature to remove device from CC-SG control
- Support of Raritan PDUs
- Support for remote IP access from the new Dominion KX III User Station
- Support for access to serial targets using the Dominion Serial Access Module (DSAM)

Dominion KX3-832

KX3-832 Photos



KX3-832 Features

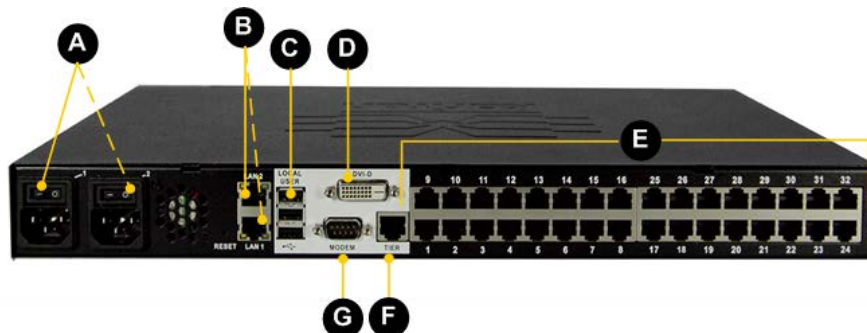


Diagram key

A	Dual Power AC 100V/240V
B	Dual 10/100/1000 Ethernet access
C	Local USB ports
D	DVI-D port

Diagram key	
E	32 KVM ports for UTP Cabling (Cat5/5e/6)
F	Tier port for tiering devices
G	Modem port for external modems

Dominion KX3-864

KX3-864 Photos



KX3-864 Features

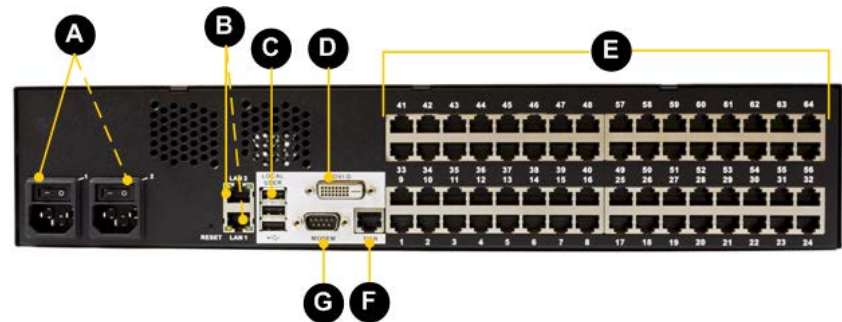


Diagram key	
A	Dual Power AC 100V/240V

Diagram key	
B	Dual 10/100/1000 Ethernet access
C	Local USB ports
D	DVI-D port
E	64 KVM ports for UTP Cabling (Cat5/5e/6)
F	Tier port for optional tiering devices
G	Modem port for optional external modems

Supported Number of Ports and Remote Users per Model

Model	Ports	Remote users
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

KX III Remote/Local Console Interfaces and User Station

Use the Remote Console interface to configure and manage the KX III over a network connection.

Use the Local Console interface to access the KX III while at the rack.

See *KX III Remote Console Interface* (on page 20), *KX III Local Console - KX III Administration Functions* (see "*KX III Local Console - Administration Functions*" on page 221) and *KX III Local Console Interface* (on page 30), respectively.

The Dominion User Station provides an alternative interface for IP access to the KX III's target servers. See *Dominion KX III User Station* (on page 360).

KX III KVM Client Applications

KX III works with -

- Active KVM Client (AKC) - Default client, Windows only. Microsoft .NET® 4.0 (or later) is required to use KX III with the Microsoft Windows®-based Active KVM Client (AKC). See *Active KVM Client (AKC) Help* (on page 301)
- Virtual KVM Client (VKC) - Java™ 1.7 is required to use the Java-based Virtual KVM Client (VKC). Java 1.8.0_40 is required to use the VKCS. Also available in a Standalone version for the Chrome browser. Java is required. See *Virtual KVM Client (VKC) Help* (see "*Virtual KVM Client (VKC and VKCs) Help*" on page 256)
- HTML KVM Client (HKC) - Runs on Linux, Mac, and Windows without .NET, in IE, Edge, Firefox, Chrome and Safari. No Java. Basic KVM features are supported. See *HTML KVM Client (HKC) Help* (on page 305).
- Mobile KVM Client (MKC) - Mobile access is provided through Mobile Access Client, which requires the use of CommandCenter Secure Gateway (CC-SG). See *Mobile KVM Client (MKC) Help* (on page 364)

KX III Online Help

KX III online help is considered your primary help resource.

KVM Client help is provided as part of KX III online help.

Online help is accompanied by the KX III Quick Setup Guide, which is included with your KX III and can be found on the Support page of

Raritan's website

(<http://www.raritan.com/support/firmware-and-documentation>).

The Support page also contains a PDF version of the end user help sections of online help, and a PDF containing the KX III administrator help sections.

See the KX III Release Notes for important information on the current release before you begin using the KX III.

To use online help, Active Content must be enabled in your browser.

Chapter 2 Get Started Using KX III

This section walks you through high-level tasks to start using KX III.

In This Chapter

Install and Configure KX III.....	10
Factory Default Login Information	10
Allow Pop-Ups.....	10
Security Warnings and Validation Messages.....	11
Installing a Certificate	12
Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional)	16
Logging In to KX III	18

Install and Configure KX III

If you have not already done so, install and configure KX III.
See the KX III Quick Setup Guide that came with the KX III device or
download it from the *Raritan Support website*
<http://www.raritan.com/support>.

Factory Default Login Information

The KX III device is shipped from the factory with the following default
settings built in:

- Username = admin
All lowercase.
This user has administrative privileges.
- Password = raritan
All lowercase.
- IP address = 192.168.0.192

**Important: For backup and business continuity purposes, it is
strongly recommended you create a backup administrator username
and password, and keep that information in a secure location.**

Allow Pop-Ups

Regardless of the browser you are using, you must allow pop-ups in
order to launch the KX III Remote Console.

Security Warnings and Validation Messages

When logging in to KX III using RSC, security warnings and application validation message may appear.

These include -

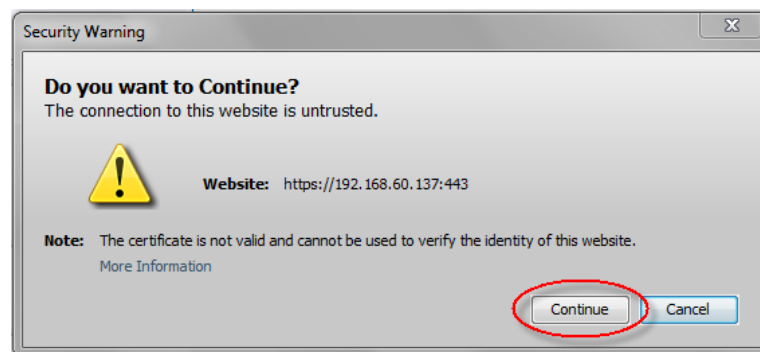
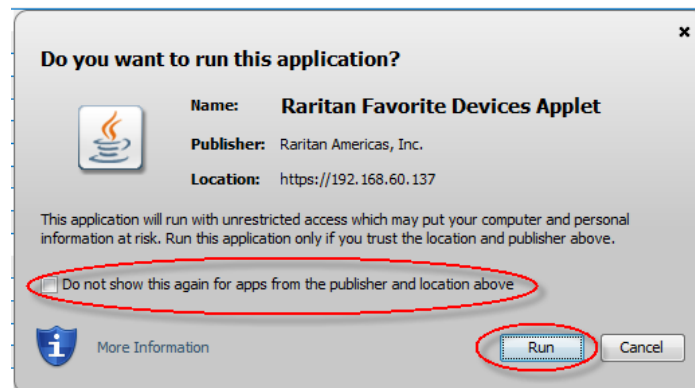
- Java™ security warnings and requests to validate KX III
See *Java Validation and Access Warning* (on page 11) and *Installing a Certificate* (on page 12)
- Additional security warnings based on your browser and security settings
See *Additional Security Warnings* (on page 12)

Java Validation and Access Warning

When logging in to KX III, Java™ 1.7 prompts you to validate KX III, and to allow access to the application.

Raritan recommends installing an SSL certificate in each KX III device in order to reduce Java warnings, and enhance security.

See *SSL Certificates* (see "*SSL and TLS Certificates*" on page 200)



Additional Security Warnings

Even after an SSL certificate is installed in the KX III, depending on your browser and security settings, additional security warnings may be displayed when you log in to KX III.

It is necessary to accept these warnings to launch the KX III Remote Console.

Reduce the number of warning messages during subsequent log ins by checking the following options on the security and certificate warning messages:

- In the future, do not show this warning
- Always trust content from this publisher

Installing a Certificate

You may be prompted by the browser to accept and validate the KX III's SSL certificate.

Depending on your browser and security settings, additional security warnings may be displayed when you log in to KX III.

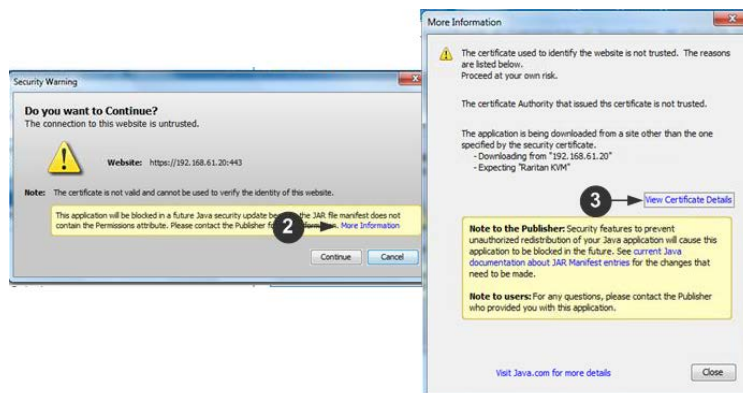
It is necessary to accept these warnings to launch the KX III Remote Console. For more information, see ***Security Warnings and Validation Messages*** (on page 11).

Two sample methods on how to install an SSL Certificate in the browser are provided here, both using Microsoft Internet Explorer 8® and Windows 7®.

Specific methods and steps depend on your browser and operating system. See your browser and operating system help for details.

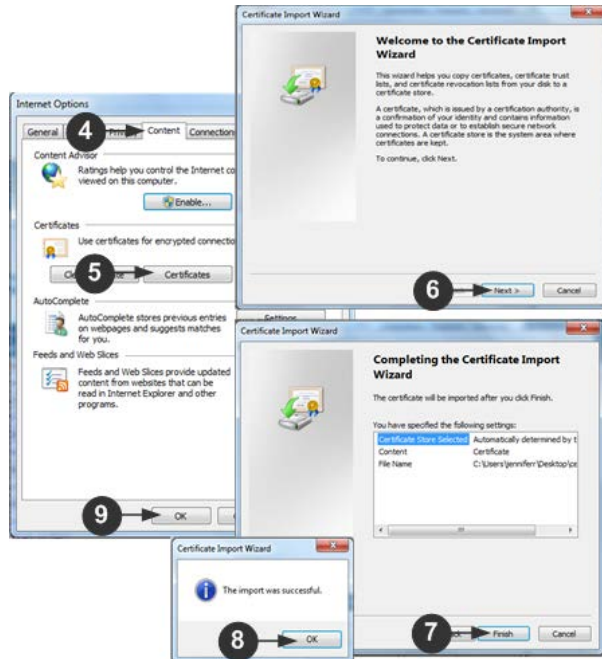
Example 1: Import the Certificate into the Browser

In this example, you import the Certificate into the browser.



1. Open an IE browser, then log in to KX III.
2. Click More Information on the first Java™ security warning.
3. Click View Certificate Details on the More Information dialog. You are prompted to install the certificate. Follow the wizard steps.

Note: If you are not prompted by the browser, manually select Tools > Internet Options to open the Internet Options dialog.

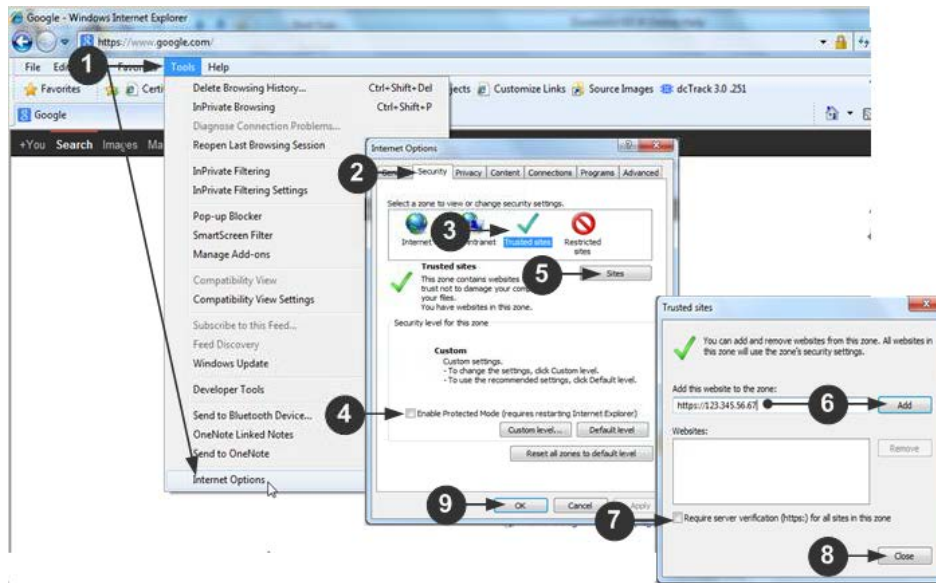


1. Click the Content tab.
2. Click Certificates.
 - File to Import - Browse to locate the Certificate
 - Certificate Store - Select the location to store the Certificate
3. Click Finish on the last step of the Wizard.

The Certificate is imported. Close the success message.
4. Click OK on the Internet Options dialog to apply the changes, then close and reopen the browser.

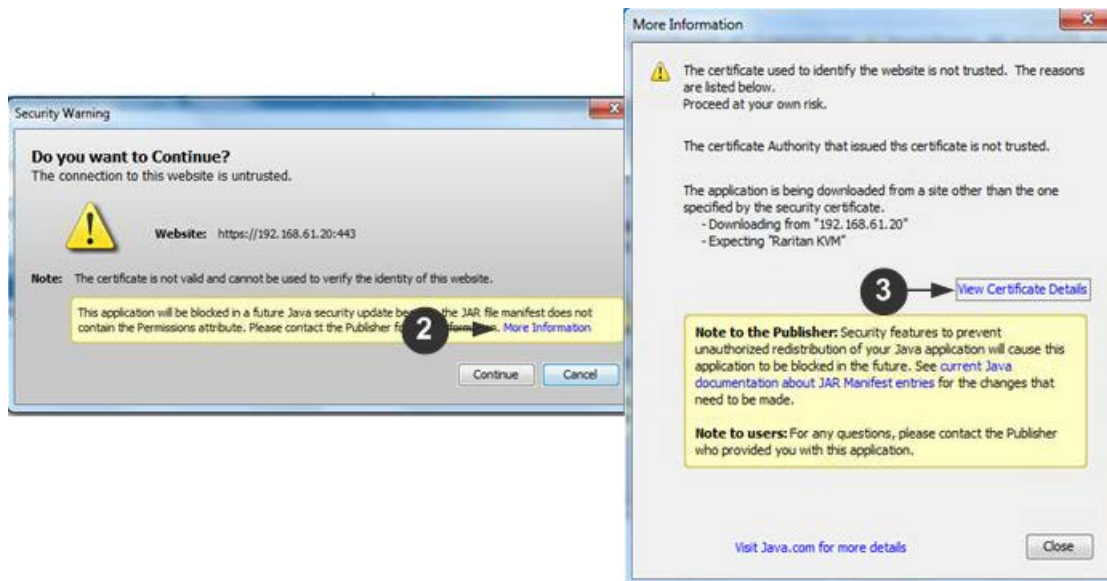
Example 2: Add the KX III to Trusted Sites and Import the Certificate

In this example, the KX III's URL is added as a Trusted Site, and the Self Signed Certificate is added as part of the process.



1. Open an IE browser, then select Tools > Internet Options to open the Internet Options dialog
2. Click the Security tab.
3. Click on Trusted Sites.
4. Disable Protected Mode, and accept any warnings.
5. Click Sites to open the Trusted Sites dialog.
6. Enter the KX III URL, then click Add.
7. Deselect server verification for the zone (if applicable).
8. Click Close.
9. Click OK on the Internet Options dialog to apply the changes, then close and reopen the browser.

Next, import the Certificate.



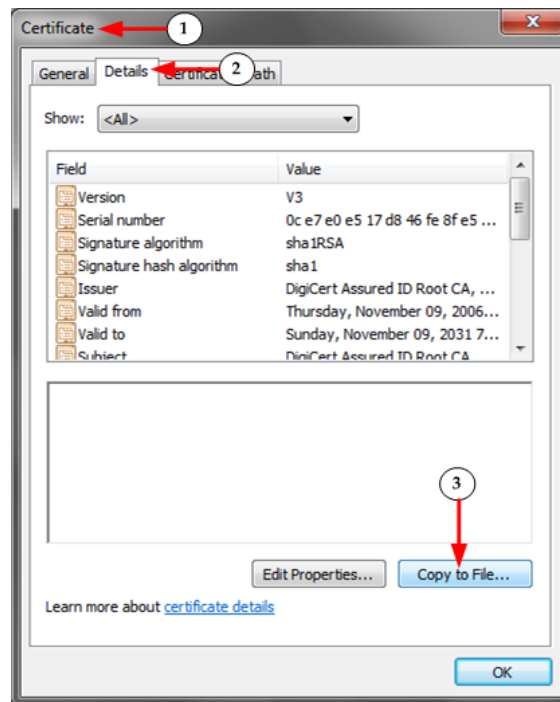
1. Open an IE browser, then log in to KX III.
2. Click More Information on the first Java™ security warning.
3. Click View Certificate Details on the More Information dialog. You are prompted to install the certificate. Follow the wizard steps.

For details see, ***Example 1: Import the Certificate into the Browser*** (on page 12).

Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional)

KX III requires an SSL certificate in either Base64-Encoded DER format or PEM format.

If you are using an SSL certificate in binary format, you cannot install it. However, you can convert your binary SSL certificate.

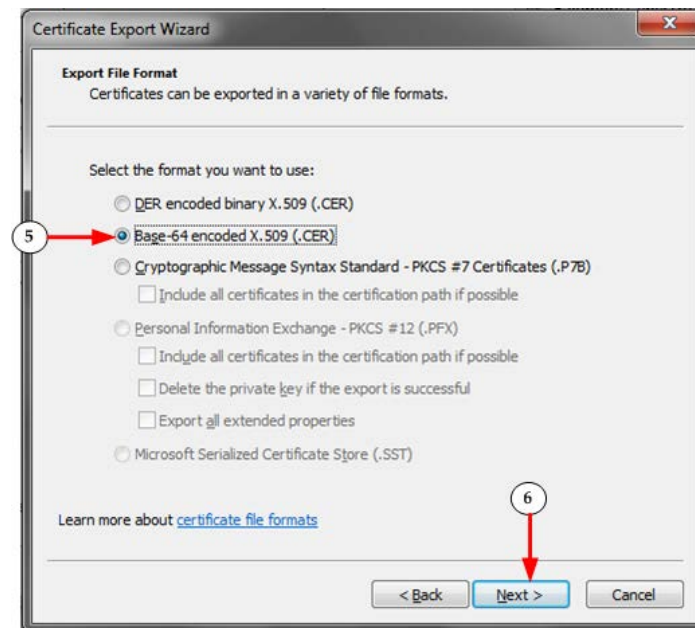


1. Locate the DEGHKVM0001.cer binary file on your Windows machine. Double-click on the DEGHKVM0001.cer file to open its Certificate dialog.
2. Click the Detail tab.

- Click "Copy to File...".



- The Certificate Export Wizard opens. Click Next to start the Wizard.



- Select "Base-64 encoded X.509" in the second Wizard dialog.
 - Click Next to save the file as a Base-64 encoded X.509.
- You can now install the certificate on your KX III.

Logging In to KX III

Log in to your KX III Remote Console from any workstation with network connectivity. Java™ 1.7 is required to use the Java-based Virtual KVM Client (VKC). Java 1.8.0_40 is required to use the VKCS. Alternatively, Microsoft .NET® 4.0 (or later) is required to use KX III with the Microsoft Windows®-based Active KVM Client (AKC).

Logging in and using KX III requires you to allow pop-ups.

For information on security warnings and validation messages, and steps to reduce or eliminate them, see ***Security Warnings and Validation Messages*** (on page 11).

If using a Dominion User Station, you must add the KX III switches you intend to access, including user credentials (login/password), on the User Station for KX III authentication.

► **To log in to the KX III via Remote Console:**

1. Launch a supported web browser, and enter the IP address assigned to the KX III.
2. A default client is launched based on your pc and browser settings. See ***KX III KVM Clients*** (on page 255). You can also choose a client by entering the URL directly. See ***KX III KVM Client Launching*** (on page 255).
3. Enter your username and password, then click Login.
4. Accept the user agreement (if applicable).
5. If security warnings appear, click to accept.

► **To add the KX III switches and user credentials to the User Station:**

1. Power on and log in to the User Station.
2. Click Main Menu > User Station Configuration > New.
3. Enter and save the following information.
 - KX III's IP address or host name
 - User credentials for logging in to the KX III

Important: If you are not the user who added KX III's to the User Station, you **MUST** click the  button for the added KX III's to save your user credentials for KX III authentication.

Chapter 3 KX III Interface and Navigation

The KX III Remote Console and the KX III Local Console are web-based graphical user interfaces.

Use the Remote Console interface to configure and manage the KX III over a network connection.

Use the Local Console interface to access the KX III while at the rack.

Access targets from either the Remote or Local console from one of the supported KVM clients.

If you have the Dominion User Station, you can also use it to access targets. See ***Dominion KX III User Station*** (on page 360).

Alternatively, access targets from your mobile device. See ***Mobile KVM Client (MKC) Help*** (on page 364).

In This Chapter

Overview	19
KX III Remote Console Interface	20
KX III Local Console Interface	30
Overview	30
KX III Installation and Configuration	30
Rack PDU (Power Strip) Outlet Control	51
USB Profiles	54
User Management.....	61
Device Management.....	87
Security Management	187
Maintenance	205
Diagnostics	217
KX III Local Console - Administration Functions.....	221
Command Line Interface (CLI)	226
Dual Video Port Groups	233

Overview

The KX III Remote Console and the KX III Local Console interfaces provide a web-based interface for device configuration and administration, as well as target server list and selection.

KX III Remote Console Interface

The KX III Remote Console is a browser-based graphical user interface that allows you to log in to KVM target servers and serial targets connected to the KX III and to remotely administer the KX III.

The KX III Remote Console provides a digital connection to your connected KVM target servers. When you log into a KVM target server using the KX III Remote Console, a Virtual KVM Client window opens.

There are many similarities among the KX III Local Console and the KX III Remote Console graphical user interfaces, and where there are differences, they are noted in the user manual. The following options are available in the KX III Remote Console but not the KX III Local Console:

- Virtual Media
- Favorites
- Backup/Restore
- Firmware Upgrade
- SSL Certificates
- Audio

Port Access Page (Remote Console Display)

After a successful login, the Port Access page opens listing all ports along with their status and availability.

Ports connected to KVM target servers (blades and standard servers) are displayed in blue. Right-click on any of these ports to open the Port Action menu. For more information, see *Port Action Menu* (on page 24).

If a KX III port has no CIM connected or is connected to a CIM with no name, a default port name of **Dominion_Dominion-KX3_Port#** is assigned to the port. Dominion_KX3 is the device model and Port# is the number of the KX III physical port.

Raritan
A brand of Legrand

Dominion® KX III

Time & Session:
January 23, 2018 19:02:02
User: admin
State: 60 min idle
Your IP: 192.168.32.61
Last Login: Jan 18, 2018 11:57:08

Device Information:
Device Name: KX3-61-16
IP Address:
192.168.61.16
192.168.60.53
1907.278.60ff:2032:20d:5dff:fe00:26f
1907.278.60ff:2031:20d:5dff:fe00:26f
Firmware: 3.5.0.5.1952
Device Model: DKX3-132
Network: LAN1 LAN2
PowerIn1: on
PowerIn2: off

Port States:
2 Ports: up
30 Ports: down
32 Ports: idle

Connected Users:
admin (192.168.32.61)
60 min idle

[Online Help](#)

Port Access

Click on the individual port name to see allowable operations.
0 / 1 Remote KVM channels currently in use.

View By Port	View By Group	View By Search	Set Scan	
No.	Name	Type	Status	Availability
1	Target 9-RSAIL-SUMLINE	Dual-VM	up	idle
2	SYSTEMTEST-OPTIPLEX	Dual-VM	up	idle
3	Dominion_KX3_Port3	Not Available	down	idle
4	Dominion_KX3_Port4	Not Available	down	idle
5	Dominion_KX3_Port5	Not Available	down	idle
6	Dominion_KX3_Port6	Not Available	down	idle
7	Dominion_KX3_Port7	Not Available	down	idle
8	Dominion_KX3_Port8	Not Available	down	idle
9	Dominion_KX3_Port9	Not Available	down	idle
10	Dominion_KX3_Port10	Not Available	down	idle
11	Dominion_KX3_Port11	Not Available	down	idle
12	Dominion_KX3_Port12	Not Available	down	idle
13	Dominion_KX3_Port13	Not Available	down	idle
14	Dominion_KX3_Port14	Not Available	down	idle
15	Dominion_KX3_Port15	Not Available	down	idle
16	Dominion_KX3_Port16	Not Available	down	idle
17	Dominion_KX3_Port17	Not Available	down	idle

Four tabs are provided on the page allowing you to view by port, view by group, view by search and scan ports. A fifth tab, View by Serial, is available when an optional DSAM is connected.

You can sort by Port Number, Port Name, Status (Up and Down), and Availability (Idle, Connected, Busy, Unavailable, and Connecting) by clicking on the column heading.

Use the Set Scan tab to scan for up to 32 targets that are connected to the KX III. See *Scanning Ports - Remote Console* (on page 375)

Tiered Devices - Port Access Page

If you are using a tiered configuration in which a base KX III device is used to access multiple other tiered devices, the tiered devices are viewed on the Port Access page by clicking on the Expand Arrow icon ► to the left of the tier device name.

Blade Chassis - Port Access Page

The blade chassis is displayed in an expandable, hierarchical list on the Port Access page, with the blade chassis at the root of the hierarchy and the individual blades labeled and displayed below the root. Use the Expand Arrow icon ► next to the root chassis to display the individual blades.

Note: To view the blade chassis in a hierarchical order, blade-chassis subtypes must be configured for the blade server chassis.

Dual Port Video Groups - Port Access Page

Dual video port groups appear on the Port Access page as Dual Port types.

The primary and secondary ports that are a part of the port group appear on the Port Access page as Dual Port(P) and Dual Port(S), respectively. For example, if the CIM type is DCIM, "DCIM Dual Port (P)" is displayed.

When you access a dual port video group from the remote client, you connect to the primary port, which opens a KVM connection window to both the primary and secondary ports of the dual port group.

Note: The dual video primary port is defined when the port group is created.

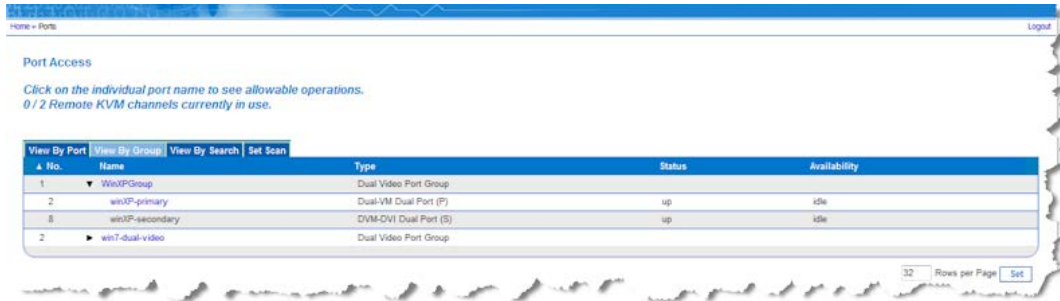
Note: You cannot remotely connect to the dual video port group by clicking on a primary port unless two KVM channels are available. If two channels are not available, the Connect link is not displayed.

Note: The Action menu is not displayed when you click on a secondary port in a dual video port group.

Note: You cannot connect to the primary port and secondary port at the same time from the Local Port.

View by Group Tab

The View by Group tab displays blade chassis, 'standard' port groups, and dual video port groups. Click the Expand Arrow icon ► next to a group to view the ports assigned to the port group.

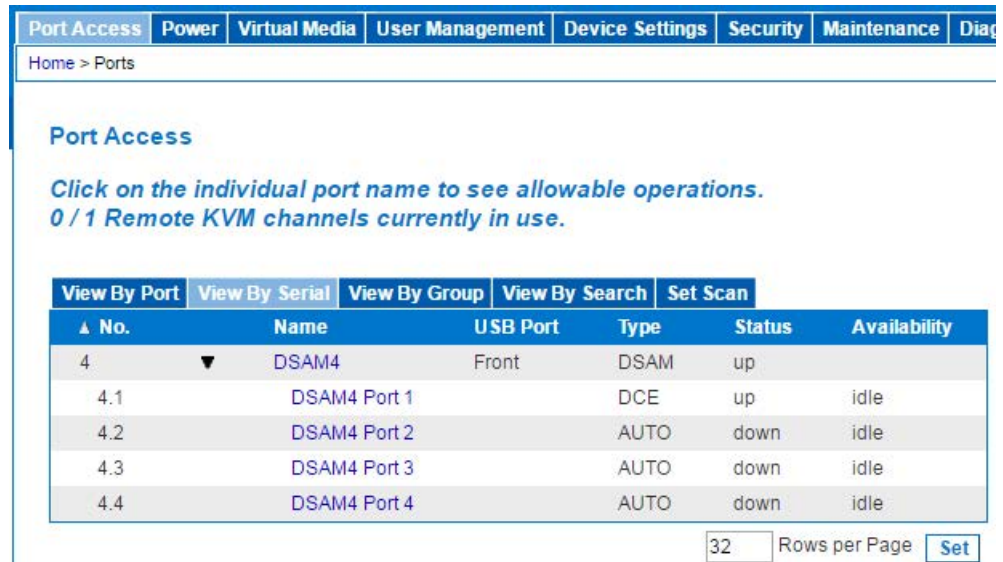


View by Search Tab

The View by Search tab allows you to search by port name. The search feature supports the use of an asterisk (*) as a wildcard, and full and partial names.

View by Serial Tab

The View By Serial tab is visible when a Dominion Serial Access Module (DSAM) is connected by USB. Up to 4 serial targets can be connected to the DSAM by USB.



Set Scan Tab

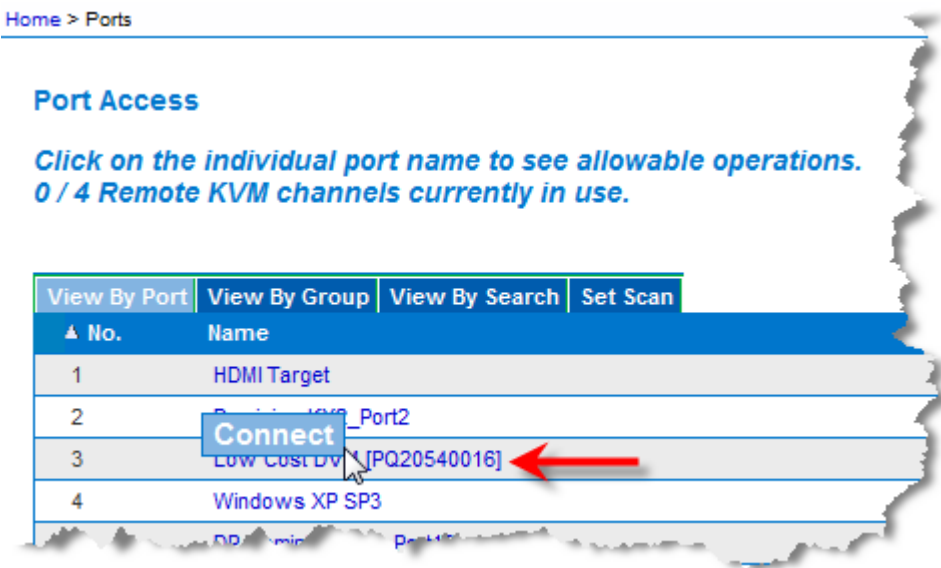
The port scanning feature is accessed from the Set Scan tab on the Port Access page. The feature allows you to define a set of targets to be scanned. Thumbnail views of the scanned targets are also available. Select a thumbnail to open that target in its Virtual KVM Client window.

See *Scanning Ports - Remote Console* (on page 375) for more information.

Port Action Menu

When you click a Port Name in the Port Access list, the Port Action menu appears.

Choose the desired menu option for that port to execute it. Note that only currently available options, depending on the port's status and availability, are listed in the Port Action menu.



Connect

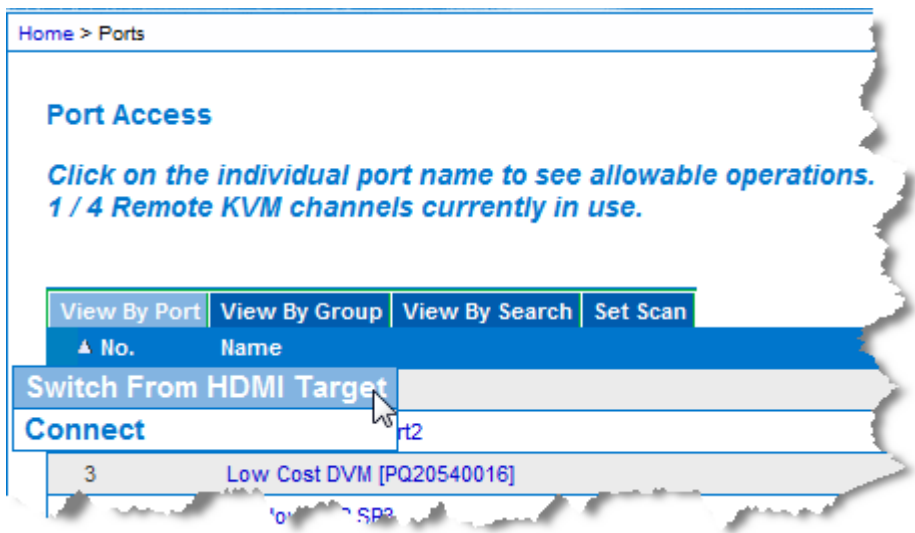
- Connect - Creates a new connection to the target server
- For the KX III Remote Console, a new Virtual KVM Client page appears.
- For the KX III Local Console, the display switches to the target server, and switches away from the local user interface.
- On the local port, the KX III Local Console interface must be visible in order to perform the switch.
- Hot key switching is also available from the local port.

Note: This option is not available from the KX III Remote Console for an available port if all connections are busy.

Switch From

- Switch From - Switches from an existing connection to the selected port (KVM target server)
This menu item is available only for KVM targets, and only when a Virtual KVM Client is opened.

Note: This menu item is not available on the KX III Local Console.



Disconnect

- Disconnect - Disconnects this port and closes the Virtual KVM Client page for this target server
This menu item is available only when the port status is up and connected, or up and busy.

Note: This menu item is not available on the KX III Local Console. The only way to disconnect from the switched target in the Local Console is to use the hot key.

[Home](#) > [Ports](#)

Port Access

Click on the individual port name to see allowable operations.
1 / 4 Remote KVM channels currently in use.

View By Port	View By Group	View By Search	Set Scan
▲ No.	Name		
1	Disconnect	get	
2	Dominion-KX2_Port2		
3			
4			

Power On

- Power On - Powers on the target server through the associated outlet

This option is visible only when there are one or more power associations to the target, and when the user has permission to operate this service.

Provided you have privileges to do so, you can manage power from the Virtual KVM Client (VKC) and Active KVM Client (AKC) as well. See ***Remote Power Management via Virtual KVM Client (VKC) or Active KVM Client (AKC)*** (see "Power Control Using VKC, VKCS, and AKC" on page 300)

Power Off

- Power Off - Powers off the target server through the associated outlets

This option is visible only when there are one or more power associations to the target, when the target power is on (port status is up), and when user has permission to operate this service.

Provided you have privileges to do so, you can manage power from the Virtual KVM Client (VKC) and Active KVM Client (AKC) as well. See ***Remote Power Management via Virtual KVM Client (VKC) or Active KVM Client (AKC)*** (see "Power Control Using VKC, VKCS, and AKC" on page 300)

Power Cycle

- Power Cycle - Power cycles the target server through the associated outlets

This option is visible only when there are one or more power associations to the target, and when the user has permission to operate this service.

Provided you have privileges to do so, you can manage power from the Virtual KVM Client (VKC) and Active KVM Client (AKC) as well. See ***Remote Power Management via Virtual KVM Client (VKC) or Active KVM Client (AKC)*** (see "Power Control Using VKC, VKCS, and AKC" on page 300)

DKX3-808 Fast Switching

DKX3-808 maintains the video connections to the servers, enabling faster connections to servers and faster switching between channels.

Some Video Settings do not apply to DKX3-808 targets:

- Automatic Color Calibration
- Video Sensing: Best possible video mode/Quick sense video mode

Left Panel

The left panel of the KX III interface contains the following information.

Note that some information is conditional - meaning it is displayed based on your role, features being used and so on. Conditional information is noted here.

Information	Description	When displayed?
Time & Session	The date and time the current session started	Always
User	Username	Always
State	The current state of the application, either idle or active. If idle, the application tracks and displays the time the session has been idle.	Always
Your IP	The IP address used to access the KX III	Always
Last Login	The last login date and time	Always
Under CC-SG Management	The IP address of the CC-SG device managing the KX III	When the KX III is being managed by CC-SG
Device Information	Information specific to the KX III you are using	Always
Device Name	Name assigned to the device	Always
IP Address	The IP address of the KX III	Always
Firmware	Current version of firmware	Always
Device Model	Model of the KX III	Always
Serial number	Serial number of the KX III	Always

Information	Description	When displayed?
Network	The name assigned to the current network	Always
PowerIn1	Status of the power 1 outlet connection. Either on or off, or Auto-detect off	Always
PowerIn2	Status of the power 2 outlet connection. Either on or off, or Auto-detect off	Always
Configured As Base or Configured As Tiered	If you are using a tiering configuration, this indicates if the KX III you are accessing is the base device or a tiered device.	When the KX III is part of a tiered configuration
Port States	The statuses of the ports being used by the KX III	Always
Connect Users	The users, identified by their username and IP address, who are currently connected to the KX III	Always
Online Help	Links to online help	Always
Favorite Devices	See <i>Managing Favorites</i> (on page 381)	When enabled
FIPS Mode	FIPS Mode: Enabled SSL Certificate: FIPS Mode Compliant	When FIPS is enabled

KX III Local Console Interface

There are many similarities among the KX III Local Console and the KX III Remote Console graphical user interfaces. Where there are differences, they are noted in the help.

For details on using the Local Console see ***KX III Local Console*** (on page 385).

Overview

Administrator Help contains information specific to KX III functions typically performed by KX III application administrators, such as installing and configuring KX III, managing user groups and users, managing security, and so on.

Administrator functions are typically performed in the KX III Remote Console and/or from the Local Console.

Functions typically performed by end users using the Virtual KVM Client or Active KVM Client, and some functions performed from the Remote Console or Local Console are described in their own sections of help.

These functions include using virtual media, configuring mouse settings, using the scan port feature, configuring video options and so on.

KX III Installation and Configuration

See the ***KX III Quick Setup Guide*** that came with your device or download it from Raritan's Support website for a quick reference to the basic, bear minimum setup steps.

Additional information and optional steps included here but not in the QSG include:

- ***Additional Supported Mouse Settings*** (on page 33)
- ***LED Statuses During KX III Boot Up*** (on page 36)
- ***Connect to a VGA Monitor (Optional)*** (on page 38)
- ***Step 6: Configuring the Keyboard Language (Optional)*** (on page 50)

Rack Mounting

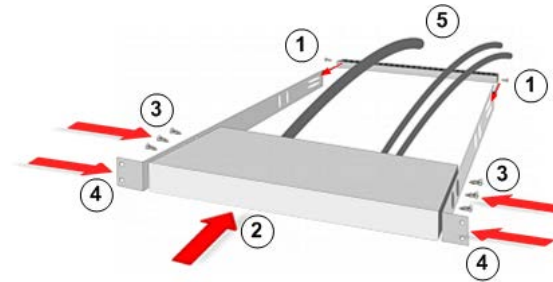
The KX III can be mounted in 1U (1.75", 4.4 cm) of vertical space in a standard 19" equipment rack.

Note: The Raritan device depicted in the rack mounting diagrams is for example purposes only and may not depict your device. The mounting instructions are specific to your device.

Forward Mount

The steps correspond to the numbers shown in the front rackmount diagrams.

1. Secure the cable-support bar to the back end of the side brackets using two of the included screws.
2. Slide the KX III between the side brackets, with its rear panel facing the cable-support bar, until its front panel is flush with the "ears" of the side brackets.
3. Secure the KX III to the side brackets using the remaining included screws (three on each side).
4. Mount the entire assembly in your rack, and secure the side brackets' ears to the rack's front rails with your own screws, bolts, cage nuts, and so on.
5. When connecting cables to the rear panel of the KX III, drape them over the cable-support bar.

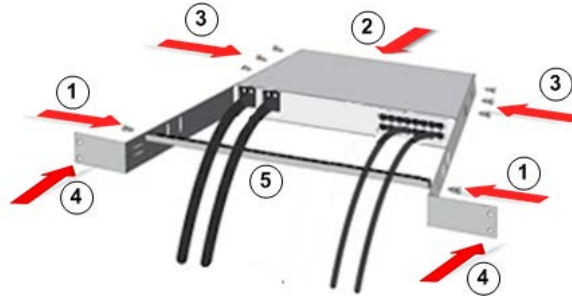


Rear Mount

The steps correspond to the numbers shown in the rear rackmount diagrams.

1. Secure the cable-support bar to the front end of the side brackets, near the side brackets' "ears," using two of the included screws.
2. Slide the KX III between the side brackets, with its rear panel facing the cable-support bar, until its front panel is flush with the back edges of the side brackets.

3. Secure the KX III to the side brackets using the remaining included screws (three on each side).
4. Mount the entire assembly in your rack and secure the side brackets' ears to the rack's front rails with your own screws, bolts, cage nuts, and so on.
5. When connecting cables to the rear panel of the user station or switch, drape them over the cable-support bar.



Factory Default Login Information

The KX III device is shipped from the factory with the following default settings built in:

- Username = admin
All lowercase.
This user has administrative privileges.
- Password = raritan
All lowercase.
- IP address = 192.168.0.192

Important: For backup and business continuity purposes, it is strongly recommended you create a backup administrator username and password, and keep that information in a secure location.

Step 1: Configuring Network Firewall Settings

TCP Port 5000

Enable remote access to KX III by allowing network and firewall communication on TCP Port 5000.

Alternatively, configure KX III to use a different TCP port, and allow that port network and firewall communication.

TCP Port 443

Allow access to TCP Port 443 (Standard HTTPS) so you can access KX III via a web browser.

TCP Port 80

Allow access to TCP Port 80 (Standard HTTP) to enable automatic redirection of HTTP requests to HTTPS.

Step 2: Configuring KVM Target Servers
Target Server Video Resolutions

For a list of supported target video server resolutions, see **KX III Supported Target Server Video Resolutions** (on page 419) in Online Help.

Mouse Settings

Raritan recommends using Absolute Mouse Synchronization to minimize mouse settings on target servers. ***Additional Supported Mouse Settings*** (on page 33).

In this mode, absolute coordinates are used to keep the client and target cursors in synch, even when the target mouse is set to a different acceleration or speed.

This mode is supported on servers with USB ports and is the default mode for virtual media CIMs.

Absolute Mouse Synchronization requires the use of a virtual media CIM

-

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

Additional Supported Mouse Settings

These settings are configured on your target operating system unless otherwise indicated.

Windows 7 and Windows Vista Mouse Settings

► Configure these mouse settings in Windows 7® and Windows Vista®:

Configure the motion settings:

- Set the mouse motion speed setting to exactly the middle speed
- Disable the "Enhanced pointer precision" option

Disable animation and fade effects:

- Animate controls and elements inside windows
- Animate windows when minimizing and maximizing
- Fade or slide menus into view
- Fade or slide ToolTips into view
- Fade out menu items after clicking

Windows XP, Windows 2003, Windows 2008 Mouse Settings

► Configure these mouse settings in Windows XP®, Windows 2003® and Windows 2008®:

Configure the Motion settings:

- Set the mouse motion speed setting to exactly the middle speed
- Disable the "Enhance pointer precision" option
- Disable the Snap To option

Disable transition effects:

- Deselect the "Use the following transition effect for menus and tooltips" option

Windows 2000 Mouse Settings

► Configure these Windows 2000® mouse settings:

Configure the Motion settings:

- Set the acceleration to None
- Set the mouse motion speed setting to exactly the middle speed

Disable transition effects:

- Deselect the "Use the following transition effect for menus and tooltips" option

Apple Mac Mouse Settings**► Configure these Apple Mac® mouse settings:**

Absolute Mouse Synchronization is required for proper mouse synchronization on KVM target servers running a Mac® operating system. In order for Absolute Mouse Synchronization to work, a virtual media CIM is required. For a list of supported CIMs, see ***Supported Computer Interface Module (CIMs) Specifications*** (on page 421).

Once you have completed your KX III installation, set the Mac USB profile. If you do not set this profile, the mouse does synch in OS X.

To do this, do one of the following:

1. Connect to the Mac target from the Raritan KVM Client.
 2. Select USB Profile > Other Profiles > Mac OS-X (10.4.9 and later).
- Or**
3. In KX III, select Device Settings > Port Configuration, then click on the target name to open the Port page.
 4. Expand 'Select USB Profiles for Port' section.
 5. Select 'Mac OS-X (10.4.9) and later' from the Available box, then click Add to add it to the Selected box.
 6. Click on 'Mac OS-X (10.4.9) and later' in the Selected box. This automatically adds it to the Preferred Profile drop-down.
 7. Select 'Mac OS-X (10.4.9) and later' from the Preferred Profile drop-down, then check the checkbox under 'Set Active Profile As Preferred Profile'.
- Click OK to apply.

Linux Mouse Settings**► Configure these Linux® mouse settings:**

- (Standard Mouse Mode only) Set the mouse acceleration to exactly 1 and set the threshold to exactly 1. Enter the following command:
`xset mouse 1 1`. This should be set for execution upon login.

Sun Solaris Mouse Settings**► Configure these Sun® Solaris™ mouse settings:**

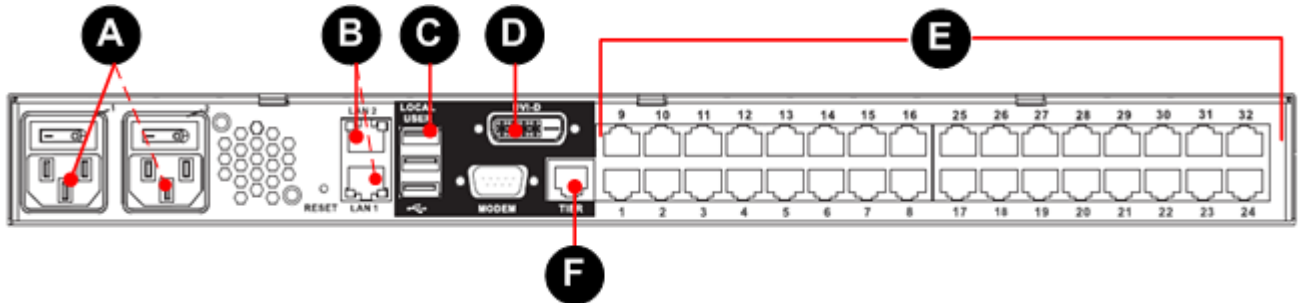
- Set the mouse acceleration value to exactly 1 and the threshold to exactly 1
- Ensure that your video card is set to a supported resolution and that its output is VGA, not composite sync

IBM AIX Mouse Settings

► **Configure these IBM AIX® mouse settings:**

- Go to the Style Manager, click on Mouse Settings and set Mouse Acceleration to 1.0 and Threshold to 3.0

Step 3: Connecting the Equipment



A: AC Power



1. Use the power cords that came with KX III. Use both cords with AC power outlets for dual-power failover protection.

Optional For details on enabling power supply autodetection from the Remote Console, see Specify Power Supply Autodetection in online help.

LED Statuses During KX III Boot Up

When you boot up the KX III, the LED lights behave as follows:

- When first powered up:
 - All Channel LEDs are on

- The Power LED is off
- At the boot phase:
 - All Channel LEDs are off
 - If both power supplies are on, the Power LED is Blue
 - If one power supply is on, the Power LED is Red

B. Network Ports

Two network ports are provided to allow for both failover and isolation modes.

Connect a standard Ethernet cable from the LAN1 network port on the KX III to an Ethernet switch, hub, or router.

If you will use failover or isolation modes, connect a standard Ethernet cable from the LAN2 network port on the KX III to an Ethernet switch, hub, or router.

See ***Choose Failover or Isolation Mode*** (on page 39) for more details.

C: Local User Port (Local Console)

► To connect the keyboard and mouse:

- Connect a USB keyboard and mouse to the respective Local User port on the back of KX III.

Use the KX III Local User port for administrative and target device access at the rack. The Local User port is required for installation and setup, but is optional for subsequent use.

D. Local DVI-D Port

A single link DVI cable is used to connect to a local DVI monitor or keyboard tray (not included with the KX III).

Connect to the DVI port on Raritan's T1700-LED or T1900-LED keyboard tray.

Use a required DVI-D to VGA converter to connect to VGA monitors.

Connect to a DVI Monitor

The local monitor must support a minimum 1024x768 resolution.

1. Connect a USB keyboard and mouse to the respective Local User ports on the back of KX III.
2. Connect a DVI cable from the DVI-D port on the back of KX III to the DVI monitor.

Connect to a VGA Monitor (Optional)

► To connect to a VGA monitor:

1. Connect a USB keyboard and mouse to the respective Local User ports on the back of the KX III.
2. Plug the DVI-D to VGA converter in to the DVI-D port on the back of the KX III, and secure it by turning the screws on each side clockwise.
3. Connect a VGA cable to the DVI-D to VGA converter, connect the other end to your VGA monitor and secure it by tightening the screws.

Note: The DVI-D to VGA converter is not included with the KX III. Some converters require a power supply. Contact Raritan Sales for information.

E. Connect Target Servers to KX III

1. Connect the keyboard, mouse and video plugs on the CIM to the corresponding ports on the target server.
2. Connect the CIM to an available target server port on the back of the KX III via a Cat5/5e/6 cable.

F. Tiering (Optional)

See ***Configuring and Enabling Tiering*** (on page 145)

G. Connect the Modem (Optional)

See ***Configuring Modem Settings*** (on page 156).

Step 4: Configuring the KX III

For the following steps, you must change the default password and assign the KX III its IP address at the Local Console.

All other steps can be performed either from the Local Console, or the KX III Remote Console via a supported web browser using the KX III's default IP address.

Java™ 1.7 is required to use the Java-based Virtual KVM Client (VKC).

Java 1.8.0_40 is required to use the VKCS.

Microsoft .NET® 4.0 (or later) is required to use KX III with the Microsoft Windows®-based Active KVM Client (AKC).

Change the Default Password

The first time you start the KX III device, you are required to change the default password.

1. Once the unit has booted, enter the default username `admin` and password `raritan`.
2. Click Login.
3. Enter the old password `raritan`, then enter and reenter a new password.
4. Passwords can be up to 64 characters in length consisting of English alphanumeric characters and special characters.
5. Click Apply.
6. Click OK on the Confirmation page.

Assign the KX III a Device Name

Open the Device Network Settings page in the KX III Remote client

Basic Network Settings

Device Name *
 Dominion51-220

IPv4 Address

IP Address 192.168.61.13	Subnet Mask 255.255.255.0
Default Gateway 192.168.61.126	Preferred DHCP Host Name

IP Auto Configuration
 DHCP
 None
 DHCP

1. Specify a meaningful Device Name for your KX III device.
Up to 32 alphanumeric and valid special characters, no spaces between characters.

Next, configure the IP address and DNS settings.

Choose Failover or Isolation Mode

Configure KX III for Dual LAN Failover Mode (on page 40)

Configure KX III for Dual LAN Isolation Mode (on page 41)

Configure KX III for Dual LAN Failover Mode

LAN1 and LAN2 share the same IP address to support automatic failover.

LAN1 is the primary port. If LAN1 fails, LAN2 is used to access KX III.

1. Select Device Settings > Network to open the Device Network Settings page.
2. Set the IP Auto Configuration to *None* in the IPv4 section.
3. Select the "Enable Automatic Failover" checkbox under LAN Interface Settings to enable failover.
4. Manually specify the network parameters by entering the Default Gateway.
5. Enter the IPv4 IP Address, if needed. The default IP address is 192.168.0.192.
6. Enter the IPv4 Subnet Mask. The default subnet mask is 255.255.255.0.
7. The LAN1 settings are applied to LAN2 if failover occurs.

The screenshot displays the 'Device Network Settings' page, divided into two main sections: 'Basic Network Settings' and 'LAN Interface Settings'.

Basic Network Settings:

- Device Name:** A text field with 'Dominion' entered.
- IPv4 Address:** A section containing:
 - IP Address:** 192.168.60.137
 - Subnet Mask:** 255.255.255.0
 - Default Gateway:** 192.168.60.126
 - IP Auto Configuration:** A dropdown menu set to 'None'.
- IPv6 Address:** A section with fields for Global/Unique IP Address, Prefix Length, Gateway IP Address, Link-Local IP Address, and Zone ID. The IP Auto Configuration dropdown is set to 'None'.
- LAN2 IPv4 Address:** A section with fields for IP Address, Subnet Mask (255.255.255.0), Default Gateway (192.168.61.126), and IP Auto Configuration (set to 'None').
- LAN2 IPv6 Address:** A section with fields for Global/Unique IP Address, Prefix Length, Gateway IP Address, Link-Local IP Address, and Zone ID. The IP Auto Configuration dropdown is set to 'None'.
- Preferred DHCP Host Name:** A text field with 'S60-137' entered.

LAN Interface Settings:

- Note:** For reliable network communication, co-ordination and LAN Switch to the same Speed and Duplex. For example, configure both Dominion and LAN Switch to Autodetect or set both to a fixed speed/duplex such as 10.
- Current LAN Interface Parameters:** autonegotiation on, 100 Mbps, full duplex, link ok.
- LAN Interface Speed & Duplex:** A dropdown menu set to 'Autodetect'.
- Current LAN2 Interface Parameters:** autonegotiation on, 1000 Mbps, full duplex, link ok.
- LAN2 Interface Speed & Duplex:** A dropdown menu set to 'Autodetect'.
- Enable Automatic Failover:** A checkbox that is checked, with a red arrow pointing to it.

8. Complete the IPv6 sections, if applicable.
9. Select the IP Auto Configuration.

If *None* is selected, you must manually specify -

- Global/Unique IP Address - this is the IP address assigned to KX III.
- Prefix Length - this is the number of bits used in the IPv6 address.
- Gateway IP Address.

Select *Router Discovery* to locate a Global or Unique IPv6 address instead of a Link-Local subnet. Once located, the address is automatically applied.

Note that the following additional, read-only information appears in this section -

- Link-Local IP Address - this address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present.
- Zone ID - Identifies the device the address is associated with.
Read-Only

10. Next, select "Use the Following DNS Server Addresses" and enter the Primary DNS Server IP Address and Secondary DNS Server IP Address. The secondary address is used if the primary DNS server connection is lost due to an outage.

Note: "Obtain DNS Server Address Automatically" and "Preferred DHCP Host Name" are only enabled when KX III is configured in DHCP mode

11. When finished, click OK. Your KX III device is now network accessible.

Configure KX III for Dual LAN Isolation Mode

Isolation mode allows you to access each LAN port independently using different IP addresses.

Failover is not supported in this mode.

1. Select Device Settings > Network to open the Device Network Settings page.

2. Set the IP Auto Configuration to *None* in the IPv4 section.
3. Ensure the "Enable Automatic Failover" checkbox is not selected.

Current LAN Interface Parameters:
autonegotiation on, 100 Mbps, full duplex, link ok

LAN Interface Speed & Duplex
Autodetect

Current LAN2 Interface Parameters:
autonegotiation on, 1000 Mbps, full duplex, link ok

LAN2 Interface Speed & Duplex
Autodetect

☐ Enable Automatic Failover

4. If needed, manually specify the network parameters by entering the Default Gateway and then complete the steps that follow.
Alternatively, if you do not want to set a static IP, see Disable or Enable DHCP in KX III.
5. Enter the IP address you want to use to connect to the KX III LAN1.
The default IP address is 192.168.0.192.
6. Enter the IPv4 Subnet Mask. The default subnet mask is 255.255.255.0.
7. In the LAN2 IPv4 section, set the IP Auto Configuration to *None*.
8. Enter the IP address you want to use to connect to the KX III LAN2.
9. Enter the LAN2 IPv4 Default Gateway and Subnet Mask.

Basic Network Settings

Device Name *

IPv4 Address

IP Address: 192.168.0.192 Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.128 IP Auto Configuration: None

IPv6 Address

Global/Unique IP Address: / Prefix Length

Gateway IP Address

Link-Local IP Address: N/A Zone ID: %1

IP Auto Configuration: None

LAN2 IPv4 Address

IP Address: 192.168.0.11 Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.15 IP Auto Configuration: None

LAN2 IPv6 Address

Global/Unique IP Address: / Prefix Length

Gateway IP Address

Link-Local IP Address: N/A Zone ID: %1

IP Auto Configuration: None

10. Complete the IPv6 sections, if applicable.
11. Select the IP Auto Configuration.
If *None* is selected, you must manually specify -

- Global/Unique IP Address - this is the IP address assigned to KX III.
- Prefix Length - this is the number of bits used in the IPv6 address.
- Gateway IP Address.

Select *Router Discovery* to locate a Global or Unique IPv6 address instead of a Link-Local subnet. Once located, the address is automatically applied.

Note that the following additional, read-only information appears in this section -

- Link-Local IP Address - this address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present.
- Zone ID - Identifies the device the address is associated with.

12. Select "Use the Following DNS Server Addresses" and enter the Primary DNS Server IP Address and Secondary DNS Server IP Address. The secondary address is used if the primary DNS server connection is lost due to an outage.

Note: "Obtain DNS Server Address Automatically" and "Preferred DHCP Host Name" are only enabled when KX III is configured in DHCP mode

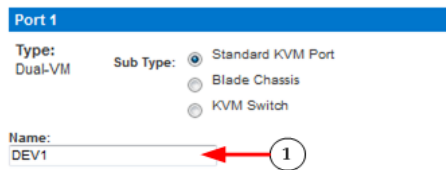
13. When finished, click OK.

Your KX III device is now accessible via the LAN1 IP address and the LAN2 IP address.

Name Your Target Servers

Connect all of the target servers if you have not already done so.

Select Device Settings > Port Configuration, then click the Port Name of the target server you want to name.



1. Enter a name for the server up to 32 alphanumeric and special characters. Click OK.

Specify Power Supply Autodetection

KX III provides dual power supplies.

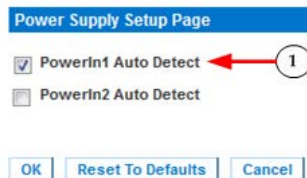
When both power supplies are used, KX III automatically detects them and notifies you of their status. Additionally, both the PowerIn1 and PowerIn2 Auto Detect checkboxes are automatically selected on the Power Supply Setup page.

If you are using only one power supply, you can enable automatic detection for only the power supply in use.

When only one power input is connected, the Power LED on the front of the KX III device is Red when the checkbox is selected for an unconnected power supply, and Blue when the checkbox is not selected for an unconnected power supply.

► To enable automatic detection for the power supply in use:

Home > Device Settings > Power Supply Setup Page

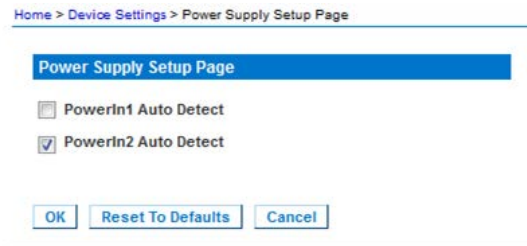


1. Select Device Settings > Power Supply Setup.

- Select the PowerIn1 Auto Detect option if you are plugging power input into power supply number one.

(The left-most power supply at the back of the device when you are facing rear of the device.)

Or



- Select the PowerIn2 Auto Detect option if you are plugging power input into power supply number two.

(The right-most power supply at the back of the device when you are facing rear of the device.)

Click OK.

Configure Date/Time Settings

The date and time settings impact SSL certificate validation if LDAPS is enabled. Configuring the date and time also ensures your audit logs will be timestamped correctly.

There are two ways to do this:

- Manually set the date and time.

The screenshot shows the 'Date/Time Settings' page in the KX III interface. The breadcrumb trail at the top reads 'Home > Device Settings > Date/Time Settings', with the last two items circled in red. The 'Time Zone' dropdown is set to '(GMT -05:00) US Eastern'. The 'Adjust for daylight savings time' checkbox is checked. The 'User Specified Time' radio button is selected. The date is set to June 15, 2015, and the time is 10:55:58. A red arrow points to the date input field. At the bottom are 'OK', 'Reset To Defaults', and 'Cancel' buttons.

- Synchronize the date and time with a Network Time Protocol (NTP) server.

The screenshot shows the 'Date/Time Settings' page in the KX III interface. The breadcrumb trail at the top reads 'Home > Device Settings > Date/Time Settings', with the last two items circled in red. The 'Time Zone' dropdown is set to '(GMT -05:00) US Eastern'. The 'Adjust for daylight savings time' checkbox is checked. The 'Synchronize with NTP Server' radio button is selected. The 'Primary Time Server' and 'Secondary Time Server' fields are empty. A red arrow points to the 'Synchronize with NTP Server' radio button. At the bottom are 'OK', 'Reset To Defaults', and 'Cancel' buttons.

1. Choose Device Settings > Date/Time to open the Date/Time Settings page.
2. Choose your time zone from the Time Zone drop-down list.

3. Adjust for daylight savings time by checking the "Adjust for daylight savings time" checkbox.
4. Choose the method to use to set the date and time:
 - User Specified Time - use this option to input the date and time manually. For the User Specified Time option, enter the date and time. For the time, use the hh:mm format (using a 24-hour clock).
 - Synchronize with NTP Server - use this option to synchronize the date and time with the Network Time Protocol (NTP) Server.
For the Synchronize with NTP Server option:
 - Enter the IP address of the Primary Time server.
 - Enter the IP address of the Secondary Time server. **Optional**

Note: If DHCP is selected for the Network Settings on the Network page, the NTP server IP address is automatically retrieved from the DHCP server by default. Manually enter the NTP server IP address by selecting the Override DHCP checkbox.

5. Click OK.

Create User Groups and Users

Note to CC-SG Users

When the KX III is controlled by CommandCenter Secure Gateway, CC-SG authenticates users and groups, except for local users requiring Local port access.

When CC-SG is controlling the KX III, local port users will be authenticated against the local user database or the remote authentication server (LDAP/LDAPS or RADIUS) configured on the KX III. They will not be authenticated against the CC-SG user database.

For additional information about CC-SG authentication, see the **CommandCenter Secure Gateway User Guide, Administrator Guide, or Deployment Guide**, which can be downloaded from the Support section of the **Raritan website** <http://www.raritan.com>.

Supported Protocols

To simplify management of usernames and passwords, the KX III provides the ability to forward authentication requests to an external authentication server. Two external authentication protocols are supported: LDAP/LDAPS and RADIUS.

Note on Microsoft Active Directory

Microsoft® Active Directory® uses the LDAP/LDAPS protocol natively, and can function as an LDAP/LDAPS server and authentication source for the KX III. If it has the IAS (Internet Authorization Server) component, a Microsoft Active Directory server can also serve as a RADIUS authentication source.

Step 5: Launching the KX III Remote Console

1. Launch a supported web browser, and enter the IP address assigned to the KX III.
2. A default client is launched based on your pc and browser settings. See *KX III KVM Clients* (on page 255). You can also choose a client by entering the URL directly. See *KX III KVM Client Launching* (on page 255).
3. Enter your username and password, then click Login.
4. Accept the user agreement (if applicable).
5. If security warnings appear, click to accept.

*Tip: If you have a Dominion KX III User Station, you can use it to remotely access the KX III target servers. See **Dominion KX III User Station** (on page 360).*

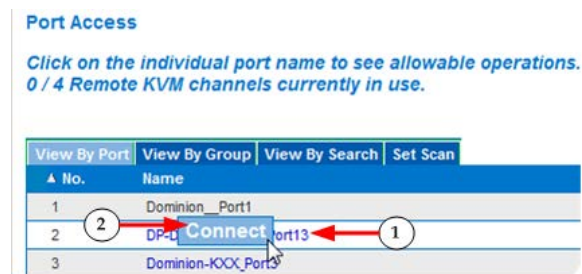
Access and Control Target Servers Remotely

The KX III Port Access page provides a list of all KX III ports.

The page also lists all of the target servers connected to the KX III along with their status and availability.

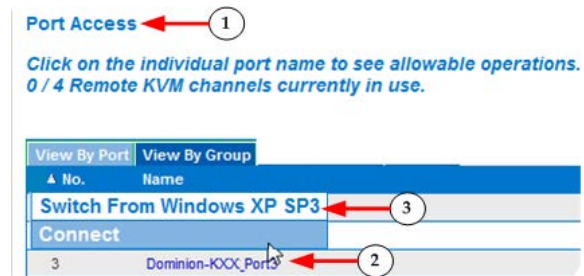
Access a Target Server from the KX III

► To access a target server:



1. On the KX III Port Access page, click the Port Name of the target you want to access. The Port Action Menu is displayed.
2. Choose Connect from the Port Action menu. A KVM window opens with a connection to the target.

Switch between Target Servers



- ① While already using a target server, access the KX III Port Access page.
- ② Click the port name of the target you want to access. The Port Action menu appears.
- ③ Choose Switch From. The new target server you selected is displayed.

DKX3-808 Fast Switching

DKX3-808 maintains the video connections to the servers, enabling faster connections to servers and faster switching between channels.

Some Video Settings do not apply to DKX3-808 targets:

- Automatic Color Calibration
- Video Sensing: Best possible video mode/Quick sense video mode

Disconnect from a Target Server

► To disconnect a target:

- On the Port Access page, click the port name of the target you want to disconnect from, then click Disconnect on the Port Action menu when it appears.

Or

- Close the client window.

Step 6: Configuring the Keyboard Language (Optional)

Note: This step is not required if you are using the US/International language keyboard.

If you are using a non-US language, the keyboard must be configured for the appropriate language.

Additionally, the keyboard language for the client machine and the KVM target servers must match.

Consult your operating system documentation for additional information about changing the keyboard layout.

Change the Keyboard Layout Code (Sun Targets)

Use this procedure if you are using a DCIM-SUSB and want to change the keyboard layout to another language.

► **To change the keyboard layout code (DCIM-SUSB only):**

①	Open a Text Editor window on the Sun™ workstation.
②	Check that the Num Lock key is active. then press the left Ctrl key and the Del key on your keyboard, or select the option "set CIM keyboard/Mouse options" from the keyboard menu. The Caps Lock light starts to blink, indicating that the CIM is in Layout Code Change mode. The text window displays: Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX).
③	Type the layout code desired (for example, 31 for the Japanese keyboard). Press Enter.
④	Shut down the device and power on once again. The DCIM-SUSB performs a reset (power cycle).
⑤	Verify that the characters are correct.

1.

Step 7: Create and Install an SSL Certificate

Raritan strongly recommends you install your own SSL Certificate in each KX III device.

This security best practice reduces the number of Java™ warning messages, and avoids man-in-the-middle attacks.

It also prevents future Java versions and browser versions from blocking access to your KX III device.

For information creating and installing SSL certificates, see **SSL Certificates** (see "**SSL and TLS Certificates**" on page 200).

Rack PDU (Power Strip) Outlet Control

Overview

You can control Raritan PX and RPC series rack PDU (power strip) outlets connected to the KX III through a D2CIM-PWR.

Once connected to the KX III, the rack PDU and its outlets are controlled from the Powerstrip page, which is accessed by clicking on the Power menu at the top of the page.

Note: If no powerstrips are connected to KX III, a message stating "No powerstrips found" is displayed in the Powerstrip Device section of page.

All of the powerstrips you have permissions to access and which are connected to KX III are listed in the Powerstrip drop-down.

Information about the currently selected powerstrip is displayed under the Powerstrip drop-down.

- Name
- Model
- Temperature
- Current Amps
- Maximum Amps
- Voltage
- Power in Watts
- Power in Volts Ampere
- Outlet Display Information:
 - Name - Named assigned to the outlet when it was configured.
 - State - On or Off status of the outlet
 - Control - Turn outlets on or off, or cycle their power
 - Association - The target ports associated with the outlet

In the case of tiered configurations, the Powerstrip page will display both rack PDUs attached to the base and tiered KX IIIs, for which the user has been granted appropriate port access permissions.

- Outlet Display Information:
 - Name - Named assigned to the outlet when it was configured.
 - State - On or Off status of the outlet
 - Control - Turn outlets on or off, or cycle their power
 - Association - The ports associated with the outlet

Home > Powerstrip Log

Operation completed successfully.

Powerstrip Device

Powerstrip: rk-power ▼ Refresh

Name: Model: Temperature: CurrentAmps: MaxAmps: Voltage: PowerIn/Watt: PowerIn/VA:
 rk-power PCR8 29 °C 0 A 0 A 118 V 3 W 0 VA

Name	State	Control	Associations
Outlet 1	on	On Off Cycle	Dominion_Port9
Outlet 2	on	On Off Cycle	
Outlet 3	on	On Off Cycle	
Outlet 4	on	On Off Cycle	
Outlet 5	on	On Off Cycle	Dominion_Port2
Outlet 6	on	On Off Cycle	
Outlet 7	on	On Off Cycle	
Outlet 8	on	On Off Cycle	

If you have privileges, you can also control power from HKC, AKC, VKC, VKCs, and the Admin client. See *Remote Power Management via Virtual KVM Client (VKC) or Active KVM Client (AKC)* (see "Power Control Using VKC, VKCS, and AKC" on page 300)

Turning Outlets On/Off and Cycling Power

► To turn an outlet on:

1. Click the Power menu to access the Powerstrip page.
2. From the Powerstrip drop-down, select the PX rack PDU (power strip) you want to turn on.
3. Click Refresh to view the power controls.
4. Click On next to the outlet you want to power on.

5. Click OK to close the Power On confirmation dialog. The outlet will be turned on and its state will be displayed as 'on'.

► **To turn an outlet off:**

1. Click Off next to the outlet you want to power off.
2. Click OK on the Power Off dialog.
3. Click OK on the Power Off confirmation dialog. The outlet will be turned off and its state will be displayed as 'off'.

► **To cycle the power of an outlet:**

1. Click Cycle next to the outlet you want to cycle. The Power Cycle Port dialog opens.
2. Click OK. The outlet will then cycle (note that this may take a few seconds).
3. Once the cycling is complete the dialog will open. Click OK to close the dialog.

USB Profiles

Overview

To broaden the KX III's compatibility with different KVM target servers, Raritan provides a standard selection of USB configuration profiles for a wide range of operating system and BIOS-level server implementations.

The Generic (default) USB profile meets the needs of the vast majority of deployed KVM target server configurations.

Additional profiles are provided to meet the specific needs of other commonly deployed server configurations (for example, Linux® and Mac OS X®).

There are also a number of profiles (designated by platform name and BIOS revision) to enhance virtual media function compatibility with the target server, for example, when operating at the BIOS level.

USB profiles are configured on the Device Settings > Port Configuration > Port page of the KX III Remote and Local Consoles.

Administrators configure the port with the USB profiles that best meet the needs of the user, and the target server configuration.

A user connecting to a KVM target server chooses among these preselected profiles in the Virtual KVM Client, depending on the operational state of the KVM target server.

For example, if the server is running Windows® operating system, it would be best to use the Generic profile.

To change settings in the BIOS menu or boot from a virtual media drive, depending on the target server model, a BIOS profile may be more appropriate.

Should none of the standard USB profiles provided by Raritan work with a given KVM target, please contact Raritan Technical Support for assistance.

CIM Compatibility

In order to make use of USB profiles, you must use a virtual media CIM with updated firmware. For a list of virtual media CIMs, see ***Supported Computer Interface Module (CIMs) Specifications*** (on page 421).

Available USB Profiles

The current release of the KX III comes with the selection of USB profiles described in the following table. New profiles are included with each firmware upgrade provided by Raritan. As new profiles are added, they will be documented in the help.

USB profile	Description
BIOS Dell® PowerEdge® 1950/2950/2970/6950/R200	Dell PowerEdge 1950/2950/2970/6950/R200 BIOS Use either this profile or 'Generic' profile for Dell PowerEdge 1950/2950/2970/6950/R200 BIOS. Restrictions: ▪ None
BIOS Dell OptiPlex™ Keyboard and Mouse Only	Dell OptiPlex BIOS Access (Keyboard and Mouse Only) Use this profile to have keyboard functionality for the Dell OptiPlex BIOS when using D2CIM-VUSB. When using the new D2CIM-DVUSB, use 'Generic' profile. Notice: ▪ Optiplex 210L/280/745/GX620 requires D2CIM-DVUSB with 'Generic' profile to support virtual media Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ No virtual media support
BIOS Dell Optiplex 790	Use this profile for Dell Optiplex 790 during BIOS operations. Warning: ▪ USB enumeration will trigger whenever Virtual Media is connected or disconnected Restrictions: ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ Absolute mouse synchronization not supported ▪ Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS Dell Optiplex 790 Keyboard Only	Use this profile for Dell Optiplex 790 when using Keyboard Macros during BIOS operations. Only keyboard is enabled with this profile. Restrictions: ▪ Mouse is disabled. ▪ Virtual CD-ROM and disk drives are disabled.

USB profile	Description
BIOS DellPowerEdge Keyboard and Mouse Only	Dell PowerEdge BIOS Access (Keyboard and Mouse Only) Use this profile to have keyboard functionality for the Dell PowerEdge BIOS when using D2CIM-VUSB. When using the new D2CIM-DVUSB, use 'Generic' profile. Notice: - PowerEdge 650/1650/1750/2600/2650 BIOS do not support USB CD-ROM and disk drives as a bootable device - PowerEdge 750/850/860/1850/2850/SC1425 BIOS requires D2CIM-DVUSB with 'Generic' profile to support virtual media - Use 'BIOS Dell PowerEdge 1950/2950/2970/6950/R200' or 'Generic' profile for PowerEdge 1950/2950/2970/6950/R200 when operating in the BIOS Restrictions: - USB bus speed limited to full-speed (12 MBit/s) - Absolute mouse synchronization™ not supported - No virtual media support
BIOS ASUS P4C800 Motherboard	Use this profile to access BIOS and boot from Virtual Media on Asus P4C800-based systems. Restrictions: - USB bus speed limited to full-speed (12 MBit/s) - Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS Generic	BIOS Generic Use this profile when Generic OS profile does not work on the BIOS. WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected. Restrictions: - USB bus speed limited to full-speed (12 MBit/s) - Absolute mouse synchronization™ not supported - Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS HP® Proliant™ DL145	HP Proliant DL145 PhoenixBIOS Use this profile for HP Proliant DL145 PhoenixBIOS during OS installation. Restrictions:

USB profile	Description
	USB bus speed limited to full-speed (12 MBit/s)
BIOS HP Compaq® DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 Use this profile to boot the HP Compaq DC7100/DC7600 series desktops from virtual media. Restrictions: Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS IBM ThinkCentre Lenovo	IBM Thinkcentre Lenovo BIOS Use this profile for the IBM® Thinkcentre Lenovo system board (model 828841U) during BIOS operations. Restrictions: - USB bus speed limited to full-speed (12 MBit/s) - Virtual CD-ROM and disk drives cannot be used simultaneously
IBM BladeCenter H with Advanced Management Module	Use this profile to enable virtual media functionality when D2CIM-VUSB or D2CIM-DVUSB is connected to the Advanced Management Module. Restrictions: Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS Lenovo ThinkPad T61 & X61	BIOS Lenovo ThinkPad T61 and X61 (boot from virtual media) Use this profile to boot the T61 and X61 series laptops from virtual media. Restrictions: USB bus speed limited to full-speed (12 MBit/s)
Generic	The generic USB profile resembles the behavior of the original KX3 release. Use this for Windows 2000® operating system, Windows XP® operating system, Windows Vista® operating system and later. Note: Microsoft no longer supports some legacy Windows OS, and using them may be a security risk. Restrictions: None
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	HP Proliant DL360/DL380 G4 (HP SmartStart CD) Use this profile for the HP Proliant DL360/DL380 G4 series server when installing OS using HP SmartStart CD. Restrictions:

USB profile	Description
	- USB bus speed limited to full-speed (12 MBit/s) - Absolute mouse synchronization™ not supported
HP Proliant DL360/DL380 G4 (Windows 2003® Server Installation)	HP Proliant DL360/DL380 G4 (Windows 2003 Server Installation) Use this profile for the HP Proliant DL360/DL380 G4 series server when installing Windows 2003 Server without the help of HP SmartStart CD. Restrictions: USB bus speed limited to full-speed (12 MBit/s)
Linux®	Generic Linux profile This is the generic Linux profile; use it for Redhat Enterprise Linux, SuSE Linux Enterprise Desktop and similar distributions. Restrictions: Absolute mouse synchronization™ not supported
BIOS Mac®	BIOS Mac Use this profile for Mac BIOS. Restrictions: - Absolute mouse synchronization™ is not supported - Virtual CD-ROM and disk drives cannot be used simultaneously If you use this USB profile, see <i>Mouse Modes when Using the Mac Boot Menu</i> (on page 60) for information mouse modes when using the Mac Boot Menu
MAC OS X® 10.4.9 (and later)	Mac OS X version 10.4.9 (and later) This profile compensates the scaling of mouse coordinates introduced in recent versions of Mac OS X. Select this if the remote and local mouse positions get out of sync near the desktop borders. Restrictions: Virtual CD-ROM and disk drives cannot be used simultaneously
RUBY Industrial Mainboard (AwardBIOS)	RUBY Industrial Mainboard (AwardBIOS) Use this profile for the RUBY-9715VG2A series industrial mainboards with Phoenix/AwardBIOS v6.00PG. Restrictions: - USB bus speed limited to full-speed (12 MBit/s) - Virtual CD-ROM and disk drives cannot be used simultaneously

USB profile	Description
Supermicro Mainboard Phoenix (AwardBIOS)	Supermicro Mainboard Phoenix AwardBIOS Use this profile for the Supermicro series mainboards with Phoenix AwardBIOS. Restrictions: Virtual CD-ROM and disk drives cannot be used simultaneously
Suse 9.2	SuSE Linux 9.2 Use this for SuSE Linux 9.2 distribution. Restrictions: - Absolute mouse synchronization™ not supported - USB bus speed limited to full-speed (12 MBit/s)
Troubleshooting 1	Troubleshooting Profile 1 - Mass Storage first - Keyboard and Mouse (Type 1) - USB bus speed limited to full-speed (12 MBit/s) - Virtual CD-ROM and disk drives cannot be used simultaneously WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected.
Troubleshooting 2	Troubleshooting Profile 2 - Keyboard and Mouse (Type 2) first - Mass Storage - USB bus speed limited to full-speed (12 MBit/s) - Virtual CD-ROM and disk drives cannot be used simultaneously WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected.
Troubleshooting 3	Troubleshooting Profile 3 - Mass Storage first - Keyboard and Mouse (Type 2) - USB bus speed limited to full-speed (12 MBit/s) - Virtual CD-ROM and disk drives cannot be used simultaneously WARNING: USB enumeration will trigger whenever virtual

USB profile	Description
	media is connected or disconnected.
Use Full Speed for Virtual Media CIM	Use Full Speed for virtual media CIM This profile resembles the behavior of the original KX3 release with Full Speed for virtual media CIM option checked. Useful for BIOS that cannot handle High Speed USB devices. Restrictions: USB bus speed limited to full-speed (12 MBit/s)
Use Full Speed for Keyboard and Mouse USB	This profile will set the Keyboard and Mouse USB interface on the Dual-VM CIM to Full Speed. Useful for devices that cannot operate properly with the Low Speed USB settings. Restrictions: USB bus speed set to full-speed (12 MBit/s) on Keyboard and Mouse USB interface

Mouse Modes when Using the Mac Boot Menu

When working with the "BIOS Mac" USB profile, to use the mouse in the Mac Boot Menu, you must use Single Mouse mode since Absolute Mouse Mode is not supported in the BIOS.

► To configure the mouse to work at the Boot menu:

1. Reboot the Mac and press the Option key during the reboot to open the Boot menu. The mouse will not respond at this point.
2. Select Single Mouse mode. The mouse now responds.

Note: Mouse speed may be slow while in Single Mouse mode.

3. Once you are out of the Boot menu and back to the OS X, exit Single Mouse mode and switch back to Absolute Mouse mode.

Selecting Profiles for a KVM Port

The KX III comes with a set of USB profiles that you can assign to a KVM port based on the characteristics of the KVM target server it connects to. You assign USB profiles to a KVM port in the Device Settings > Port Configuration > Port page in either the KX III Remote or Local Console.

Administrators designates the profiles that are most likely to be needed for a specific target. These profiles are then available for selection via Virtual KVM Client (VKC). If a profile has not been made available, you can access any of the available profiles by selecting USB Profile > Other Profiles.

Assigning USB profiles to a KVM port makes those profiles available to a user when connected to a KVM target server. If required, the user can select a USB profile from the USB Profile menu in Virtual KVM Client (VKC).

For information about assigning USB profiles to a KVM port, see *Configuring USB Profiles (Port Page)* (on page 137).

User Management

User Groups

The KX III stores an internal list of all user profiles and user groups to determine access authorization and permissions. This information is stored internally in an encrypted format.

All users must be authenticated to access KX III.

KX III can be configured to authenticate users locally and/or remotely using LDAP/LDAPS or RADIUS. Remote user authentication is processed before local authentication if remote authentication is enabled.

Every KX III is delivered with three default user groups. These groups cannot be deleted:

User	Description
Admin	Users that are members of this group have full administrative privileges. The original, factory-default user is a member of this group and has the complete set of system privileges. In addition, the Admin user must be a member of the Admin group.
Unknown	This is the default group for users who are authenticated externally using LDAP/LDAPS or RADIUS or who are unknown to the system. If the external LDAP/LDAPS or RADIUS server does not

User	Description
	identify a valid user group, the Unknown group is used. In addition, any newly created user is automatically put in this group until assigned to another group.
Individual Group	An individual group is essentially a “group” of one. That is, the specific user is in its own group, not affiliated with other real groups. Individual groups can be identified by the “@” in the Group Name. The individual group allows a user account to have the same rights as a group.

Up to 254 user groups can be created in the KX III.

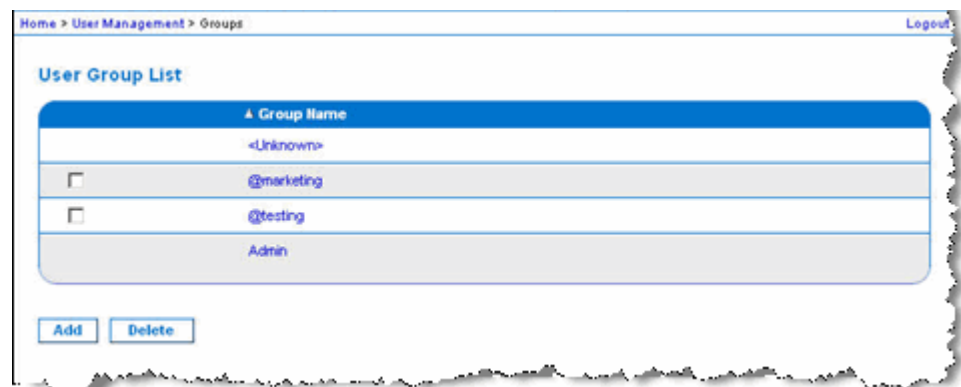
User Group List

User groups are used with local and remote authentication (via RADIUS or LDAP/LDAPS). It is a good idea to define user groups before creating individual users since, when you add a user, you must assign that user to an existing user group.

The User Group List page displays a list of all user groups, which can be sorted in ascending or descending order by clicking on the Group Name column heading. From the User Group List page, you can also add, modify, or delete user groups.

► To list the user groups:

- Choose User Management > User Group List. The User Group List page opens.



Relationship Between Users and Groups

Users belong to a group and groups have privileges. Organizing the various users of your KX III into groups saves time by allowing you to manage permissions for all users in a group at once, instead of managing permissions on a user-by-user basis.

You may also choose not to associate specific users with groups. In this case, you can classify the user as “Individual.”

Upon successful authentication, the appliance uses group information to determine the user's permissions, such as which server ports are accessible, whether rebooting the appliance is allowed, and other features.

Adding a New User Group

► To add a new user group:

1. Select User Management > Add New User Group or click Add on the User Group List page.
2. Type a descriptive name for the new user group into the Group Name field (up to 64 characters).
3. Select the checkboxes next to the permissions you want to assign to all of the users belonging to this group. See ***Setting Permissions*** (on page 64)
4. Specify the server ports and the type of access for each user belonging to this group. See ***Setting Port Permissions*** (on page 66)
5. Set the IP ACL. This feature limits access to the KX III device by specifying IP addresses. It applies only to users belonging to a specific group, unlike the IP Access Control list feature that applies to all access attempts to the device (and takes priority). See ***Group-Based IP ACL (Access Control List)*** (on page 67) **Optional**

6. Click OK.

Home > User Management > Group

Group

Group Name *

▼ Permissions

- ☐ Device Access While Under CC-SG Management
- ☐ Device Settings
- ☐ Diagnostics
- ☐ Maintenance
- ☐ PC-Share
- ☐ Security
- ☐ User Management

► Port Permissions

▼ IP ACL

Rule #	Starting IP	Ending IP	Action
			ACCEPT ▼

Append Insert Replace Delete

OK Cancel

Setting Permissions

Important: Selecting the User Management checkbox allows the members of the group to change the permissions of all users, including their own. Carefully consider granting these permissions.

Permission	Description
Device Access While Under CC-SG Management	Allows users and user groups with this permission to directly access the KX III. The KX III is accessed using an IP address when Local Access is enabled for the device in CC-SG. The device can be accessed from HKC, VKC/VKCs, and AKC. When a device is accessed directly while it is under CC-SG management, access and connection activity is logged on the KX III. User

Permission	Description
	authentication is performed based on KX III authentication settings. Note: The Admin user group has all permissions by default.
Device Settings	Network settings, date/time settings, port configuration (channel names, power associations), event management (SNMP, Syslog), virtual media file server setups.
Diagnostics	Network interface status, network statistics, ping host, trace route to host, KX III diagnostics.
Maintenance	Backup and restore database, firmware upgrade, reboot. Factory reset is available from the local console only.
Modem	Permission to use the modem to connect to the KX III device.
PC-Share	Simultaneous access to the same target by multiple users. If you are using a tiered configuration in which a base KX III device is used to access multiple, additional tiered devices, all devices must share the same PC-Share setting.
Security	SSL certificate, security settings (VM Share, PC-Share), IP ACL.
User Management	User and group management, remote, authentication (LDAP/LDAPS/RADIUS), login settings. If you are using a tiered configuration in which a base KX III device is used to access multiple other tiered devices, user, user group and remote authentication settings must be consistent across all devices.

Setting Port Permissions

For each server port, you can specify the access type the group has, as well as the type of port access to the virtual media and the power control. Please note that the default setting for all permissions is Deny.

Port access	
option	Description
Deny	Denied access completely
View	View the video (but not interact with) the connected target server.
Control	Control the connected target server. Control must be assigned to the group if VM and power control access will also be granted. In order for all users in a user group to see KVM switches that are added, each user must be granted Control access. If they don't have this permission and a KVM switch is added at a later time, they will not be able to see the switches. Control access must be granted for audio or smart card related controls to be active.

VM access	
option	Description
Deny	Virtual media permission is denied altogether for the port.
Read-Only	Virtual media access is limited to read access only.
Read-Write	Complete access (read, write) to virtual media.

Power control access

option	Description
Deny	Deny power control to the target server
Access	Full permission to power control on a target server

For blade chassis, the port access permission will control access to the URLs that have been configured for that blade chassis. The options are Deny or Control. In addition, each blade housed within the chassis has its own independent Port Permissions setting.

If you are using a tiered configuration in which a base KX III device is used to access multiple other tiered devices, the tiered device enforces individual port control levels. See *Configuring and Enabling Tiering* (on page 145) for more information on tiering.

Setting Permissions for an Individual Group**► To set permissions for an individual user group:**

1. Locate the group from among the groups listed. Individual groups can be identified by the @ in the Group Name.
2. Click the Group Name. The Group page opens.
3. Select the appropriate permissions.
4. Click OK.

Group-Based IP ACL (Access Control List)

Important: Exercise caution when using group-based IP access control. It is possible to be locked out of your KX III if your IP address is within a range that has been denied access.

This feature limits a user's access to the KX III by allowing you to assign them to a group that can only access the device through specific IP addresses.

This feature applies only to users belonging to the specific group. This is unlike the IP Access Control List feature that applies to all access attempts to the device. IP access control takes priority over group-based IP ACL and is processed first.

Important: The IP address 127.0.0.1 is used by the KX III Local Port and cannot be blocked.

Use the IP ACL section of the Group page to add, insert, replace, and delete IP access control rules on a group-level basis.

► **To add (append) rules:**

1. Type the starting IP address in the Starting IP field.
2. Type the ending IP address in the Ending IP field.
3. Choose the action from the available options:
 - Accept - IP addresses set to Accept are allowed access to the KX III device.
 - Drop - IP addresses set to Drop are denied access to the KX III device.
4. Click Append. The rule is added to the bottom of the rules list. Repeat steps 1 through 4 for each rule you want to enter.

► **To insert a rule:**

1. Enter a rule number (#). A rule number is required when using the Insert command.
2. Enter the Starting IP and Ending IP fields.
3. Choose the action from the Action drop-down list.
4. Click Insert. If the rule number you just typed equals an existing rule number, the new rule is placed ahead of the existing rule and all rules are moved down in the list.

► **To replace a rule:**

1. Specify the rule number you want to replace.
2. Type the Starting IP and Ending IP fields.
3. Choose the Action from the drop-down list.
4. Click Replace. Your new rule replaces the original rule with the same rule number.

► **To delete a rule:**

1. Specify the rule number you want to delete.
2. Click Delete.

3. When prompted to confirm the deletion, click OK.

Important: ACL rules are evaluated in the order in which they are listed. For instance, in the example shown here, if the two ACL rules were reversed, Dominion would accept no communication at all.

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

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

Tip: The rule numbers allow you to have more control over the order in which the rules are created.

Modifying an Existing User Group

Note: All permissions are enabled for the Admin group and cannot be changed.

► To modify an existing user group:

1. From the Group page, change the appropriate fields and set the appropriate permissions.
2. Set the Permissions for the group. Select the checkboxes before the permissions you want to assign to all of the users belonging to this group. See **Setting Permissions** (on page 64).
3. Set the Port Permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). See **Setting Port Permissions** (on page 66).
4. Set the IP ACL (optional). This feature limits access to the KX III device by specifying IP addresses. See **Group-Based IP ACL (Access Control List)** (on page 67).
5. Click OK.

► To delete a user group:

Important: If you delete a group with users in it, the users are automatically assigned to the <unknown> user group.

Tip: To determine the users belonging to a particular group, sort the User List by User Group.

1. Choose a group from among those listed by checking the checkbox to the left of the Group Name.
2. Click Delete.
3. When prompted to confirm the deletion, click OK.

Users

Users must be granted user names and passwords to gain access to the KX III. This information is used to authenticate users attempting to access your KX III.

Up to 254 users can be created for each user group.

If you are using a tiered configuration in which a base KX III device is used to access multiple other tiered devices, users will need permission to access the base device and permissions to access each individual tiered device (as needed).

When users log on to the base device, each tiered device is queried and the user can access each target server they have permissions to. See ***Configuring and Enabling Tiering*** (on page 145) for more information on tiering.

Adding a New User

*Note: Since you must assign a user to an existing user group when you add them, it is a good idea to define user groups before creating KX III users. See ***Adding a New User Group*** (on page 63).*

From the User page, you can add new users, modify user information, and reactivate users that have been deactivated*.

Note: A user can be deactivated when the number of failed login attempts has exceeded the maximum login attempts set in the Security Settings page. See *Security Settings*** (on page 187).*

► To add a new user:

1. Select User Management > Add New User or click Add on the User List page.
2. Type a unique name in the Username field, up to 16 characters.
3. Type the person's full name in the Full Name field, up to 64 characters.

4. Type a password in the Password field and retype the password in the Confirm Password field, up to 64 characters.
5. Choose the group from the User Group drop-down list.

If you do not want to associate this user with an existing User Group, select Individual Group from the drop-down list. For more information about permissions for an Individual Group, see ***Setting Permissions for an Individual Group*** (on page 67).

6. To activate the new user, leave the Active checkbox selected. Click OK.

View the KX III Users List

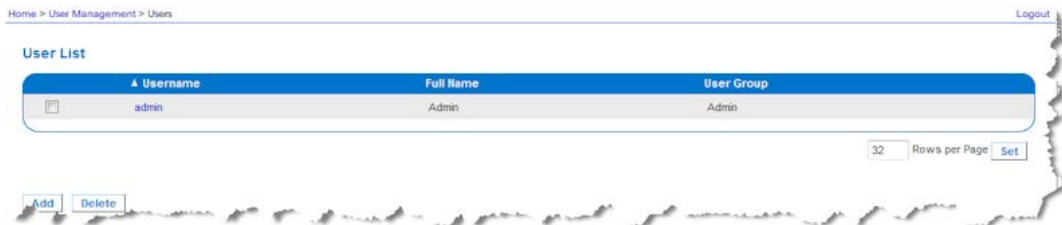
The User List page displays a list of all users including their user name, full name, and user group. The list can be sorted on any of the columns by clicking on the column name. From the User List page, you can add, modify, or delete users.

KX III users with User Management privileges can disconnect users from ports or log them off (force log off) as needed. See *Disconnecting Users from Ports* (on page 72) and *Logging Users Off the KX III (Force Logoff)* (on page 73) respectively.

To view the target ports each user is connected to, see *View Users by Port* (on page 71).

► To view the list of users:

- Choose User Management > User List. The User List page opens.



View Users by Port

The User By Ports page lists all authenticated local and remote users and ports they are being connected to. Only permanent connections to ports are listed. Ports being accessed when scanning for ports are not listed.

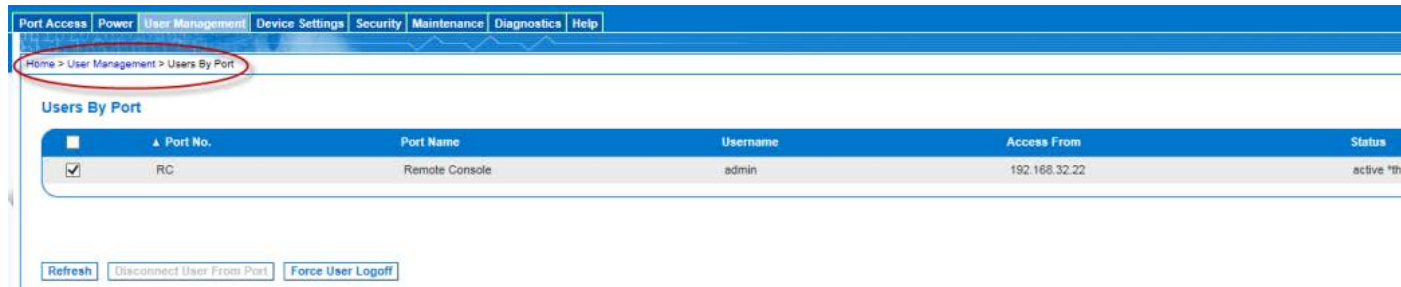
If the same user is logged on from more than one client, their username appears on the page for each connection they have made. For example, if a user has logged on from two (2) different clients, their name is listed twice.

This page contains the following user and port information:

- Port Number - port number assigned to the port the user is connected to
- Port Name - port name assigned to the port the user is connected to

Note: If user is not connected to a target, 'Local Console' or 'Remote Console' is displayed under the Port Name.

- Username - username for user logins and target connections
 - Access From - IP address of client PC accessing the KX III
 - Status - current Active or Inactive status of the connection
- **To view users by port:**
- Choose User Management > User by Port. The Users by Port page opens.



Disconnecting Users from Ports

Disconnecting users disconnects them from the target port *without* logging them off of KX III.

This is unlike the force user logoff KX III function that disconnects users from the target port and logs them off of KX III. See ***Logging Users Off the KX III (Force Logoff)*** (on page 73) for information.

If the "Disconnect User from Port" is disabled, the user is not logged on to the port at the current time.

1. Choose User Management > Users by Port. The Users by Port page opens.
2. Select the checkbox next to the username of the person you want to disconnect from the target.
3. Click "Disconnect User from Port".
4. Click OK on the confirmation message to disconnect the user.
5. A confirmation message is displayed to indicate that the user was disconnected.

Logging Users Off the KX III (Force Logoff)

If you are an administrator, you are able to log off any authenticated user who is logged on to the KX III. Users can also be disconnected at the port level. See *Disconnecting Users from Ports* (on page 72).

► To log a user off the KX III:

1. Choose User Management > Users by Port. The Users by Port page opens.
2. Select the checkbox next to the username of the person you want to disconnect from the target.
3. Click Force User Logoff.
4. Click OK on the Logoff User confirmation message.

Modifying an Existing User

► To modify an existing user:

1. Open the User List page by choosing User Management > User List.
2. Locate the user from among those listed on the User List page.
3. Click the user name. The User page opens.
4. On the User page, change the appropriate fields. See *Adding a New User* (on page 70) for information about how to get access the User page.
5. To delete a user, click Delete. You are prompted to confirm the deletion.
6. Click OK.

Authentication Settings

Authentication is the process of verifying that a user is who he says he is. Once a user is authenticated, the user's group is used to determine his system and port permissions. The user's assigned privileges determine what type of access is allowed. This is called authorization.

When the KX III is configured for remote authentication, the external authentication server is used primarily for the purposes of authentication, not authorization.

If you are using a tiered configuration in which a base KX III device is used to access multiple other tiered devices, the base device and the tiered devices must use the same authentication settings.

From the Authentication Settings page you can configure the type of authentication used for access to your KX III.

Note: When remote authentication (LDAP/LDAPS or RADIUS) is selected, if the user is not found, the local authentication database will also be checked.

► To configure authentication:

1. Choose User Management > Authentication Settings. The Authentication Settings page opens.
2. Choose the option for the authentication protocol you want to use (Local Authentication, LDAP/LDAPS, or RADIUS). Choosing the LDAP option enables the remaining LDAP fields; selecting the RADIUS option enables the remaining RADIUS fields.
3. If you choose Local Authentication, proceed to step 6.
4. If you choose LDAP/LDAPS, read the section entitled Implementing LDAP Remote Authentication for information about completing the fields in the LDAP section of the Authentication Settings page.
5. If you choose RADIUS, read the section entitled Implementing RADIUS Remote Authentication for information about completing the fields in the RADIUS section of the Authentication Settings page.
6. Click OK to save.

► To return to factory defaults:

- Click Reset to Defaults.

Implementing LDAP/LDAPS Remote Authentication

Lightweight Directory Access Protocol (LDAP/LDAPS) is a networking protocol for querying and modifying directory services running over TCP/IP. A client starts an LDAP session by connecting to an LDAP/LDAPS server (the default TCP port is 389). The client then sends operation requests to the server, and the server sends responses in turn.

Reminder: Microsoft Active Directory functions natively as an LDAP/LDAPS authentication server.

► To use the LDAP authentication protocol:

1. Click User Management > Authentication Settings to open the Authentication Settings page.
2. Select the LDAP radio button to enable the LDAP section of the page.
3. Click the  icon to expand the LDAP section of the page.

Server Configuration

4. In the Primary LDAP Server field, type the IP address or DNS name of your LDAP/LDAPS remote authentication server (up to 256 characters). When the Enable Secure LDAP option is selected and the Enable LDAPS Server Certificate Validation option is selected, the DNS name must be used to match the CN of LDAP server certificate.
5. In the Secondary LDAP Server field, type the IP address or DNS name of your backup LDAP/LDAPS server (up to 256 characters). When the Enable Secure LDAP option is selected, the DNS name must be used. Note that the remaining fields share the same settings with the Primary LDAP Server field. **Optional**
6. Type of External LDAP Server: Select the external LDAP/LDAPS server. Choose from among the options available:
 - Generic LDAP Server.
 - Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
7. Type the name of the Active Directory Domain if you selected Microsoft Active Directory. For example, *acme.com*. Consult your Active Directive Administrator for a specific domain name.
8. In the User Search DN field, enter the Distinguished Name of where in the LDAP database you want to begin searching for user information. Up to 64 characters can be used. An example base search value might be: *cn=Users,dc=raritan,dc=com*. Consult your authentication server administrator for the appropriate values to enter into these fields.

9. Enter the Distinguished Name of the Administrative User in the DN of Administrative User field (up to 64 characters). Complete this field if your LDAP server only allows administrators to search user information using the Administrative User role. Consult your authentication server administrator for the appropriate values to type into this field. An example DN of Administrative User value might be:

cn=Administrator,cn=Users,dc=testradius,dc=com.

Optional

10. If you entered a Distinguished Name for the Administrative User, you must enter the password that will be used to authenticate the Administrative User's DN against the remote authentication server. Enter the password in the Secret Phrase field and again in the Confirm Secret Phrase field (up to 128 characters).

Authentication Settings

☐ Local Authentication

☒ LDAP

☐ RADIUS

▼ LDAP

Server Configuration

Primary LDAP Server

192.168.59.187

Secondary LDAP Server (optional)

192.168.51.214

Type of External LDAP Server

Microsoft Active Directory ▼

Active Directory Domain

testradius.com

User Search DN

cn=users,dc=testradius,dc=com

DN of Administrative User (optional)

cn=Administrator,cn=users,dc=testrac

Secret Phrase of Administrative User

••••••••

Confirm Secret Phrase

LDAP/Secure LDAP

11. For an encrypted connection, select the Enable Secure LDAP checkbox to use SSL, or select the Enable StartTLS checkbox to use StartTLS. Both options enable the Enable LDAPS Server Certificate Validation checkbox.
 - For an unsecured connection, do not enable Secure LDAP or StartTLS. The default port for unsecured connections is 389. Use the standard LDAP TCP port or specify another port.
 - SSL is a cryptographic protocol that allows KX III to communicate securely with the LDAP/LDAPS server. The default Secure LDAP port is 636, or you may specify another port. This field is used only when Enable Secure LDAP is selected.
 - StartTLS is a command that upgrades an unsecured connection to a secure connection using SSL/TLS. StartTLS does not require a specific port. The standard LDAP port 389 is default.
12. Select the Enable LDAPS Server Certificate Validation checkbox to use the previously uploaded root CA certificate file to validate the certificate provided by the server. If you do not want to use the previously uploaded root CA certificate file, leave this checkbox deselected. Disabling this function is the equivalent of accepting a certificate that has been signed by an unknown certifying authority. This checkbox is only available when the Enable Secure LDAP checkbox has been enabled.

Note: When the Enable LDAPS Server Certificate Validation option is selected, in addition to using the Root CA certificate for validation, the server hostname must match the common name provided in the server certificate.

13. If needed, upload the Root CA Certificate File. This field is enabled for secured connections only. Consult your authentication server administrator to get the CA certificate file in Base64 encoded X-509 format for the LDAP/LDAPS server. Use Browse to navigate to the certificate file. If you are replacing a certificate for the LDAP/LDAPS server with a new certificate, you must reboot the KX III in order for the new certificate to take effect.

LDAP / Secure LDAP
☐ Enable Secure LDAP ☐ Enable StartTLS
Port

Secure LDAP Port

☐ Enable LDAPS Server Certificate Validation
Root CA Certificate File

Note: Reboot device after certificate file is uploaded.
No LDAP Certificate has been uploaded.

Test LDAP Server Access

14. To test the LDAP configuration, enter the login name and password in the "Login for testing" and "Password for testing" fields. Click Test.

The test login name and password should be the pair you entered to access the KX III. It is also username and password the LDAP server uses to authenticate you.

The KX III then tests the LDAP configuration from the Authentication Settings page. This is helpful due to the complexity sometimes encountered when configuring the LDAP server and KX III for remote authentication.

Once the test is completed, you will see a success message or a detailed error message. In a successful test, group information retrieved from the remote LDAP server is also displayed.

The screenshot shows a dialog box titled "Test LDAP Server Access". Inside the dialog, there are two text input fields. The first is labeled "Login for testing" and the second is labeled "Password for testing". Below these two fields is a button labeled "Test".

Returning User Group Information from Active Directory Server

The KX III supports user authentication to Active Directory® (AD) without requiring that users be defined locally on the KX III. This allows Active Directory user accounts and passwords to be maintained exclusively on the AD server. Authorization and AD user privileges are controlled and administered through the standard KX III policies and user group privileges that are applied locally to AD user groups.

IMPORTANT: If you are an existing Raritan, Inc. customer, and have already configured the Active Directory server by changing the AD schema, the KX III still supports this configuration and you do not need to perform the following operations. See [Updating the LDAP Schema](#) for information about updating the AD LDAP/LDAPS schema.

► To enable your AD server on the KX III:

1. Using the KX III, create special groups and assign proper permissions and privileges to these groups. For example, create groups such as KVM_Admin and KVM_Operator.
2. On your Active Directory server, create new groups with the same group names as in the previous step.
3. On your AD server, assign the KX III users to the groups created in step 2.
4. From the KX III, enable and configure your AD server properly. See [Implementing LDAP/LDAPS Remote Authentication](#).

Important Notes

- Group Name is case sensitive.
- The KX III provides the following default groups that cannot be changed or deleted: Admin and <Unknown>. Verify that your Active Directory server does not use the same group names.
- If the group information returned from the Active Directory server does not match the KX III group configuration, the KX III automatically assigns the group of <Unknown> to users who authenticate successfully.
- If you use a dialback number, you must enter the following case-sensitive string: *msRADIUSCallbackNumber*.
- Based on recommendations from Microsoft, Global Groups with user accounts should be used, not Domain Local Groups.

Implementing RADIUS Remote Authentication

Remote Authentication Dial-in User Service (RADIUS) is an AAA (authentication, authorization, and accounting) protocol for network access applications.

► To use the RADIUS authentication protocol:

1. Click User Management > Authentication Settings to open the Authentication Settings page.
2. Click the RADIUS radio button to enable the RADIUS section of the page.
3. Click the  icon to expand the RADIUS section of the page.
4. In the Primary Radius Server and Secondary Radius Server fields, type the IP address of your primary and optional secondary remote authentication servers, respectively (up to 256 characters).
5. In the Shared Secret fields, type the server secret used for authentication (up to 128 characters).
The shared secret is a character string that must be known by both the KX III and the RADIUS server to allow them to communicate securely. It is essentially a password.
6. The Authentication Port default is port is 1812 but can be changed as required.
7. The Accounting Port default port is 1813 but can be changed as required.
8. The Timeout is recorded in seconds and default timeout is 1 second, but can be changed as required.

The timeout is the length of time the KX III waits for a response from the RADIUS server before sending another authentication request.

9. The default number of retries is 3 Retries.
This is the number of times the KX III will send an authentication request to the RADIUS server.
10. Choose the Global Authentication Type from among the options in the drop-down list:
 - PAP - With PAP, passwords are sent as plain text. PAP is not interactive. The user name and password are sent as one data package once a connection is established, rather than the server sending a login prompt and waiting for a response.
 - CHAP - With CHAP, authentication can be requested by the server at any time. CHAP provides more security than PAP.
11. Click OK to save.

► **Test Connection:**

Test Connection

Username for testing

Password for testing

1. Enter the login name and password in the "Login for testing" and "Password for testing" fields.
 - The test login name and password should be the pair you entered to access the KX III that the RADIUS server uses to authenticate you.
 - The KX III then tests the configuration from the Authentication Settings page. This is helpful due to the complexity sometimes encountered when configuring the RADIUS server and KX III for remote authentication.
2. Once the test is completed, you will see a success message or a detailed error message. In a successful test, group information retrieved from the remote RADIUS server is also displayed.

Cisco ACS 5.x for RADIUS Authentication

If you are using a Cisco ACS 5.x server, after you have configured the KX III for RADIUS authentication, complete the following steps on the Cisco ACS 5.x server.

Note: The following steps include the Cisco menus and menu items used to access each page. Please refer to your Cisco documentation for the most up to date information on each step and more details on performing them.

- Add the KX III as a AAA Client (**Required**) - Network Resources > Network Device Group > Network Device and AAA Clients
- Add/edit users (**Required**) - Network Resources > Users and Identity Stores > Internal Identity Stores > Users
- Configure Default Network access to enable CHAP Protocol (**Optional**) - Policies > Access Services > Default Network Access
- Create authorization policy rules to control access (**Required**) - Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
 - Dictionary Type: RADIUS-IETF
 - RADIUS Attribute: Filter-ID
 - Attribute Type: String
 - Attribute Value: Raritan:G{KVM_Admin} (where KVM_Admin is group name created locally on Dominion KVM Switch). Case sensitive.
- Configure Session Conditions (Date and Time) (**Required**) - Policy Elements > Session Conditions > Date and Time
- Configure/create the Network Access Authorization Policy (**Required**) - Access Policies > Access Services > Default Network Access>Authorization

Returning User Group Information via RADIUS

When a RADIUS authentication attempt succeeds, the KX III determines the permissions for a given user based on the permissions of the user's group.

Your remote RADIUS server can provide these user group names by returning an attribute, implemented as a RADIUS FILTER-ID. The FILTER-ID should be formatted as follows: Raritan:G{*GROUP_NAME*} where *GROUP_NAME* is a string denoting the name of the group to which the user belongs.

Raritan:G{*GROUP_NAME*}:D{Dial Back Number}

where *GROUP_NAME* is a string denoting the name of the group to which the user belongs and Dial Back Number is the number associated with the user account that the KX III modem will use to dial back to the user account.

RADIUS Communication Exchange Specifications

The KX III sends the following RADIUS attributes to your RADIUS server:

Attribute	Data
Log in	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-IP-Address (4)	The IP address for the KX III.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
User-Password(2)	The encrypted password.
Accounting-Request(4)	
Acct-Status (40)	Start(1) - Starts the accounting.
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP address for the KX III.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

Attribute	Data
Log out	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - Stops the accounting
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP address for the KX III.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

RADIUS Using RSA SecurID Hardware Tokens

KX III supports RSA SecurID Hardware Tokens used with a RADIUS server for two factor authentication

Users will specify their RADIUS password followed by the token ID without a delimiter between.

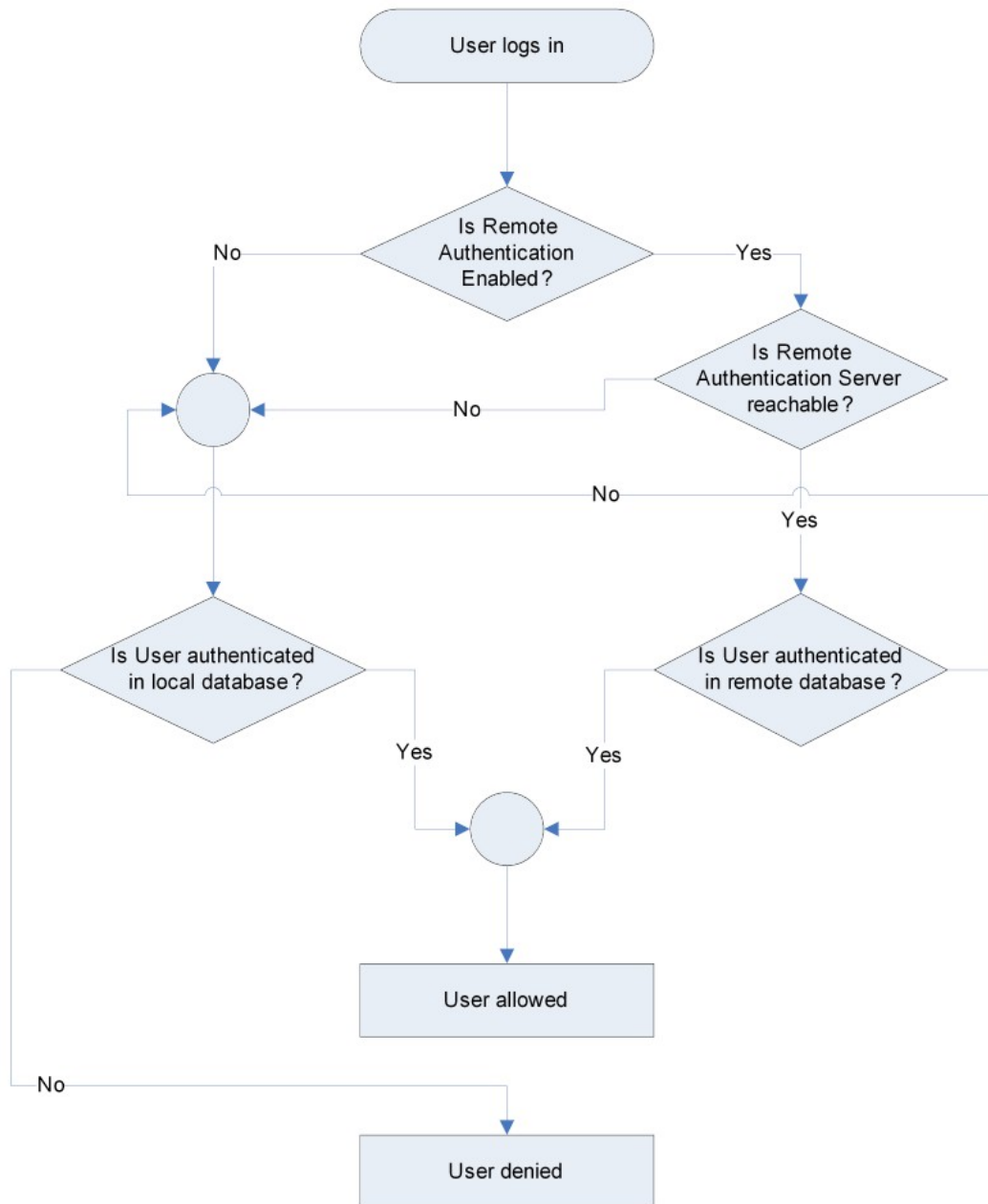
► **For example:**

- password = apple
- token = 1234
- User enters: apple1234

Or, configure the RADIUS server to use only hardware token and no passwords. Users will specify the token ID only.

User Authentication Process

Remote authentication follows the process specified in the flowchart below:

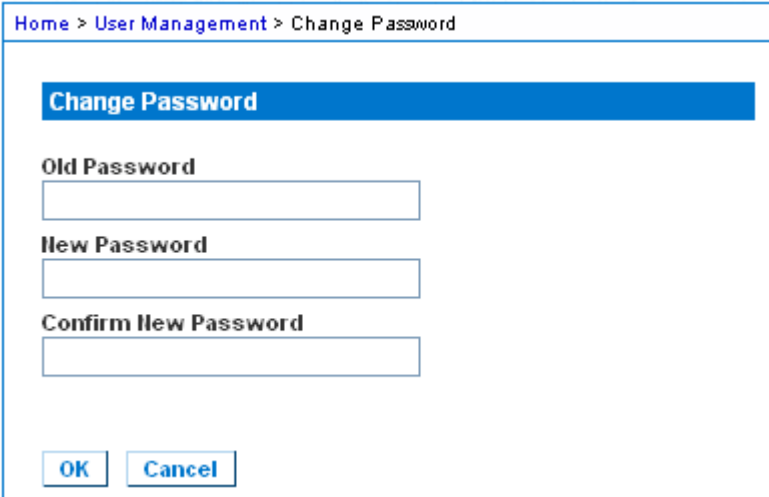


Changing a Password

► **To change your KX III password:**

1. Choose User Management > Change Password. The Change Password page opens.
2. Type your current password in the Old Password field.
3. Type a new password in the New Password field. Retype the new password in the Confirm New Password field. Passwords can be up to 64 characters in length and can consist of English alphanumeric characters and special characters.
4. Click OK.
5. You will receive confirmation that the password was successfully changed. Click OK.

*Note: If strong passwords are in use, this page displays information about the format required for the passwords. For more information about passwords and strong passwords, see **Strong Passwords** (on page 190) in online help.*



The screenshot shows a web browser window with the address bar displaying 'Home > User Management > Change Password'. The main content area has a blue header bar with the text 'Change Password'. Below this, there are three text input fields labeled 'Old Password', 'New Password', and 'Confirm New Password'. At the bottom of the form, there are two buttons: 'OK' and 'Cancel'.

Device Management

Network Settings

Choose Failover or Isolation Mode

Configure KX III for Dual LAN Failover Mode (on page 40)

Configure KX III for Dual LAN Isolation Mode (on page 41)

Configure KX III for Dual LAN Failover Mode

LAN1 and LAN2 share the same IP address to support automatic failover.

LAN1 is the primary port. If LAN1 fails, LAN2 is used to access KX III.

1. Select Device Settings > Network to open the Device Network Settings page.
2. Set the IP Auto Configuration to *None* in the IPv4 section.
3. Select the "Enable Automatic Failover" checkbox under LAN Interface Settings to enable failover.
4. Manually specify the network parameters by entering the Default Gateway.
5. Enter the IPv4 IP Address, if needed. The default IP address is 192.168.0.192.
6. Enter the IPv4 Subnet Mask. The default subnet mask is 255.255.255.0.

7. The LAN1 settings are applied to LAN2 if failover occurs.

Basic Network Settings

Device Name *
 Domain

IPv4 Address

IP Address: 192.168.60.137 Subnet Mask: 255.255.255.0
 Default Gateway: 192.168.60.126 IP Auto Configuration: None

☐ **IPv6 Address**

Global/Unique IP Address / Prefix Length
 Gateway IP Address
 Link-Local IP Address: N/A Zone ID: %1
 IP Auto Configuration: None

LAN2 IPv4 Address

IP Address: Subnet Mask: 255.255.255.0
 Default Gateway: 192.168.61.126 IP Auto Configuration: None

☐ **LAN2 IPv6 Address**

Global/Unique IP Address / Prefix Length
 Gateway IP Address
 Link-Local IP Address: N/A Zone ID: %1
 IP Auto Configuration: None

Preferred DHCP Host Name
 S60-137

LAN Interface Settings

Note: For reliable network communication, configure both the LAN Switch and LAN Switch to the same Speed and Duplex. For example, configure both the LAN Switch and LAN Switch to Autodetect or set both to a fixed speed/duplex such as 10

Current LAN Interface Parameters:
 autonegotiation on, 100 Mbps, full duplex, link ok

LAN Interface Speed & Duplex
 Autodetect

Current LAN2 Interface Parameters:
 autonegotiation on, 1000 Mbps, full duplex, link ok

LAN2 Interface Speed & Duplex
 Autodetect

☒ Enable Automatic Failover

8. Complete the IPv6 sections, if applicable.

9. Select the IP Auto Configuration.

If *None* is selected, you must manually specify -

- Global/Unique IP Address - this is the IP address assigned to KX III.
- Prefix Length - this is the number of bits used in the IPv6 address.
- Gateway IP Address.

Select *Router Discovery* to locate a Global or Unique IPv6 address instead of a Link-Local subnet. Once located, the address is automatically applied.

Note that the following additional, read-only information appears in this section -

- Link-Local IP Address - this address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present.
- Zone ID - Identifies the device the address is associated with. Read-Only

- Next, select "Use the Following DNS Server Addresses" and enter the Primary DNS Server IP Address and Secondary DNS Server IP Address. The secondary address is used if the primary DNS server connection is lost due to an outage.

Note: "Obtain DNS Server Address Automatically" and "Preferred DHCP Host Name" are only enabled when KX III is configured in DHCP mode

- When finished, click OK. Your KX III device is now network accessible.

Configure KX III for Dual LAN Isolation Mode

Isolation mode allows you to access each LAN port independently using different IP addresses.

Failover is not supported in this mode.

- Select Device Settings > Network to open the Device Network Settings page.
- Set the IP Auto Configuration to *None* in the IPv4 section.
- Ensure the "Enable Automatic Failover" checkbox is not selected.

- If needed, manually specify the network parameters by entering the Default Gateway and then complete the steps that follow.
Alternatively, if you do not want to set a static IP, see Disable or Enable DHCP in KX III.
- Enter the IP address you want to use to connect to the KX III LAN1. The default IP address is 192.168.0.192.

6. Enter the IPv4 Subnet Mask. The default subnet mask is 255.255.255.0.
7. In the LAN2 IPv4 section, set the IP Auto Configuration to *None*.
8. Enter the IP address you want to use to connect to the KX III LAN2.
9. Enter the LAN2 IPv4 Default Gateway and Subnet Mask.

The screenshot shows the 'Basic Network Settings' window. It contains several sections for configuring network settings. The 'IPv4 Address' section for LAN1 has fields for IP Address (192.168.0.137), Subnet Mask (255.255.255.0), Default Gateway (192.168.0.128), and IP Auto Configuration (None). The 'LAN2 IPv4 Address' section has fields for IP Address (192.168.0.11), Subnet Mask (255.255.255.0), Default Gateway (192.168.0.15), and IP Auto Configuration (None). There are also sections for IPv6 Address and LAN2 IPv6 Address, each with fields for Global/Unique IP Address, Prefix Length, Gateway IP Address, Link-Local IP Address, Zone ID, and IP Auto Configuration.

10. Complete the IPv6 sections, if applicable.
11. Select the IP Auto Configuration.

If *None* is selected, you must manually specify -

- Global/Unique IP Address - this is the IP address assigned to KX III.
- Prefix Length - this is the number of bits used in the IPv6 address.
- Gateway IP Address.

Select *Router Discovery* to locate a Global or Unique IPv6 address instead of a Link-Local subnet. Once located, the address is automatically applied.

Note that the following additional, read-only information appears in this section -

- Link-Local IP Address - this address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present.
- Zone ID - Identifies the device the address is associated with.
Read-Only

12. Select "Use the Following DNS Server Addresses" and enter the Primary DNS Server IP Address and Secondary DNS Server IP Address. The secondary address is used if the primary DNS server connection is lost due to an outage.

Note: "Obtain DNS Server Address Automatically" and "Preferred DHCP Host Name" are only enabled when KX III is configured in DHCP mode

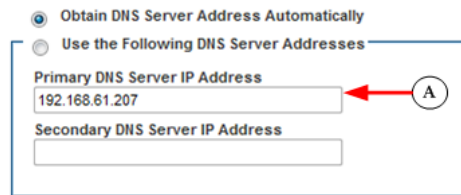
13. When finished, click OK.

Your KX III device is now accessible via the LAN1 IP address and the LAN2 IP address.

Configure the DNS Settings

1. Do one of the following to configure DNS -
 - "Obtain DNS Server Address Automatically"

- "Use the Following DNS Server Addresses"



☒ Obtain DNS Server Address Automatically
☐ Use the Following DNS Server Addresses

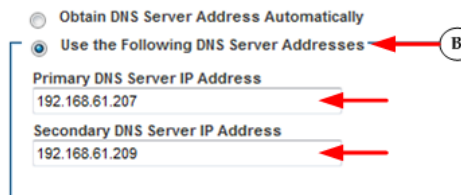
Primary DNS Server IP Address
192.168.61.207

Secondary DNS Server IP Address

- a. Select "Obtain DNS Server Address Automatically" if DHCP is selected.

The DNS information is then provided by the DHCP server that is used.

When finished, click OK. Your KX III device is now network accessible.



☐ Obtain DNS Server Address Automatically
☒ Use the Following DNS Server Addresses

Primary DNS Server IP Address
192.168.61.207

Secondary DNS Server IP Address
192.168.61.209

- b. Enter the following information if the "Use the Following DNS Server Addresses" is selected -

- Primary DNS Server IP Address
- Secondary DNS Server IP Address

These secondary DNS address is used if the primary DNS server connection is lost due to an outage.

Even if DHCP is selected in the IPv4 section, enter the primary and secondary addresses since these addresses are used to connect to the DNS server.

When finished, click OK.

View and Edit LAN Interface Settings

Choose Device Settings > Network to open the Network Settings page.
The LAN Interface Settings are in the right column.

The current LAN and LAN2 parameter settings are identified.

Device SettingsSecurityMaintenanceDiagnosticsHelp

LAN Interface Settings

Note: For reliable network communication, configure the Dominion KX3 and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX3 and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.

Current LAN Interface Parameters:
autonegotiation on, 100 Mbps, full duplex, link ok

LAN Interface Speed & Duplex
Autodetect

Current LAN2 Interface Parameters:
autonegotiation on, 1000 Mbps, full duplex, link ok

LAN2 Interface Speed & Duplex
Autodetect

☐ Enable Automatic Failover

Bandwidth Limit
No Limit

Device SettingsSecurityMaintenanceDiagnosticsHelp

LAN Interface Settings

Note: For reliable network communication, configure the Dominion KX3 and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX3 and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.

Current LAN Interface Parameters:
autonegotiation on, 100 Mbps, full duplex, link ok

LAN Interface Speed & Duplex
Autodetect

Current LAN2 Interface Parameters:
autonegotiation on, 1000 Mbps, full duplex, link ok

LAN2 Interface Speed & Duplex
Autodetect

☐ Enable Automatic Failover

Bandwidth Limit
No Limit

Raritan
A brand of  legrand

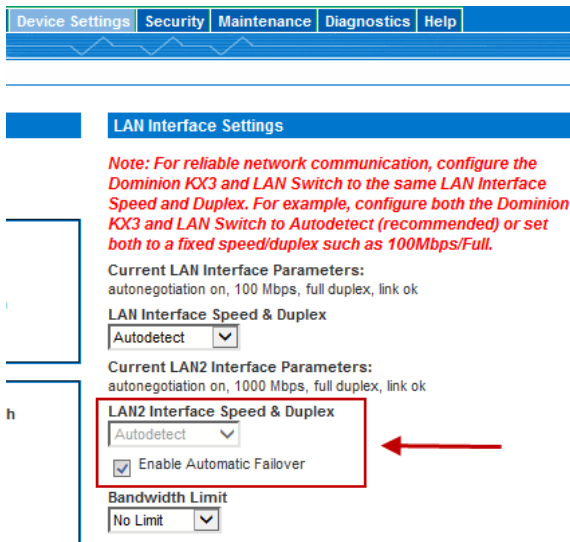
93

- 1 For each LAN, choose the LAN Interface Speed & Duplex from the following options:
 - Autodetect (default option)
 - 10 Mbps/Half - Both KX III device LEDs blink
 - 10 Mbps/Full - Both KX III device LEDs blink
 - 100 Mbps/Half - Yellow KX III device LED blinks
 - 100 Mbps/Full - Yellow KX III device LED blinks
 - 1000 Mbps/Full (gigabit) - Green KX III device LED blinks
 - Half-duplex provides for communication in both directions, but only one direction at a time (not simultaneously).
 - Full-duplex allows communication in both directions simultaneously.

Note: Occasionally there are problems running at 10 Mbps in either half or full duplex. If you are experiencing problems, try another speed and duplex setting.

See **Network Speed Settings** (on page 427) for more information.

Click OK to apply the setting.



- 2 Selecting the Enable Automatic Failover checkbox allows the KX III to automatically recover its network connection.
To do this, it uses the second network port if the active network port fails.

See **Configure KX III for Dual LAN Failover Mode** (on page 40).

Note: Because a failover port is not activated until after a failover has actually occurred, Raritan recommends that you do not monitor the port or only monitor the port after a failover occurs.

Click OK to apply the setting.

Device Settings Security Maintenance Diagnostics Help

LAN Interface Settings

Note: For reliable network communication, configure the Dominion KX3 and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX3 and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.

Current LAN Interface Parameters:
autonegotiation on, 100 Mbps, full duplex, link ok

LAN Interface Speed & Duplex
Autodetect

Current LAN2 Interface Parameters:
autonegotiation on, 1000 Mbps, full duplex, link ok

LAN2 Interface Speed & Duplex
Autodetect

☒ Enable Automatic Failover

Bandwidth Limit
No Limit

- 3 Change the Bandwidth Limit, if needed. The default is No Limit.
This sets the maximum amount of bandwidth that can be consumed by the KX III device (for all sessions).

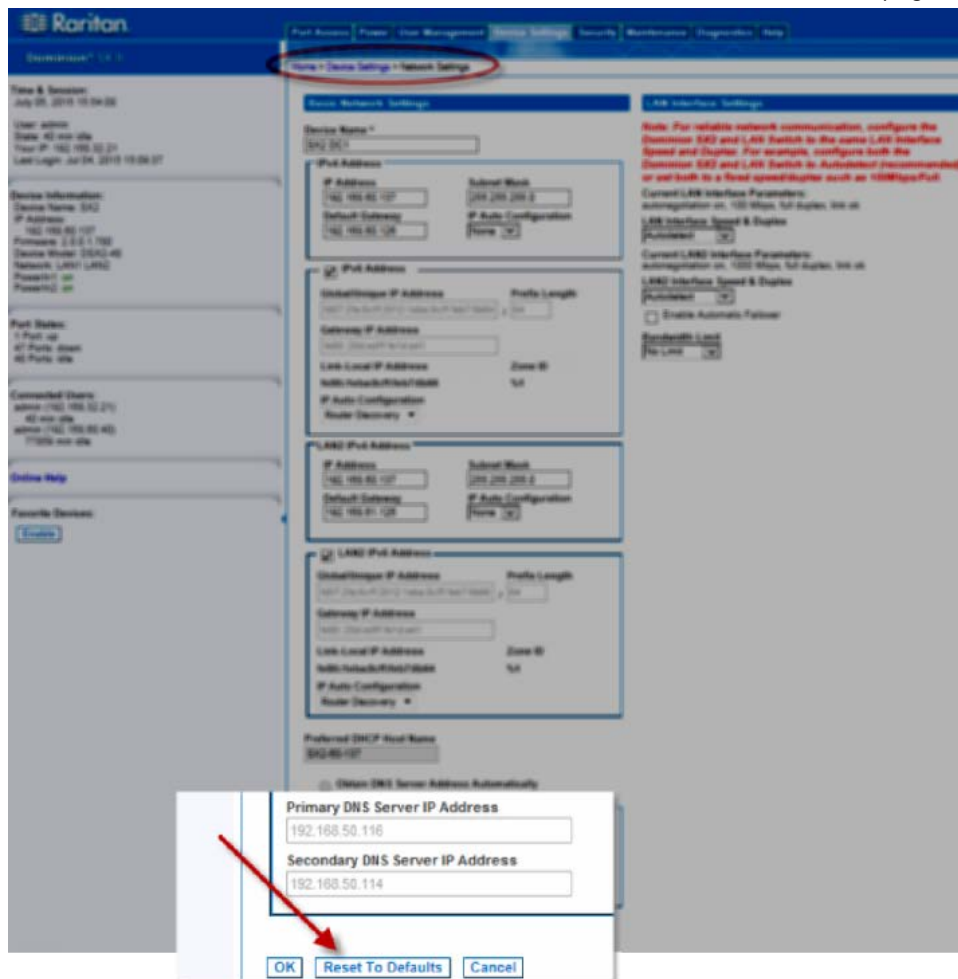
Note: Lower bandwidth may result in slower performance.

Click OK to apply the setting.

Reset Network Settings to Factory Defaults

1. Select Device Management > Network to open the Network Settings page.

- Click "Reset to Defaults" at the bottom of the page.



Configuring Ports

Access the Port Configuration Page

► To access a port configuration:

- Choose Device Settings > Port Configuration. The Port Configuration Page opens.

This page is initially displayed in port number order, but can be sorted on any of the fields by clicking on the column heading.

- Click the Port Name for the port you want to edit.
 - For KVM ports, the Port page for KVM and blade chassis ports is opened.

Port Name

If a KX III port has no CIM connected or is connected to a CIM with no name, a default port name of **Dominion_KX3_Port#** is assigned to the port. Dominion_KX3 is the device model and Port# is the number of the KX III physical port.

When a CIM is attached to the KX III, the CIM name will be used for the port.

Home > Device Settings > Port Configuration

Logout

Port Configuration

▲ No.	Name	Type
1	VM_Transfer2	DVM-HDMI
2	w7 selenium	Dual-VM
3	KX3-SYS'	DVM-DVI
4	ThinBlackline_target	DVM-DVI
5	Dominion_KX3_Port5	Not Available
6	Dominion_KX3_Port6	Not Available
7	Dominion_KX3_Port7	Not Available

To rename a port with a status of Not Available, do one of the following:

- Rename the port, and select 'Persist name on Next CIM Insertion'. When a CIM is attached, the name that has been assigned will be copied into the CIM.
- Reset the port, including the name, to factory defaults by selecting 'Reset to Defaults'. When a CIM is attached, the CIM name will be used.

Note: Do not use apostrophes for the Port (CIM) Name.

After you have renamed the port, use the Reset to Default function at any time to return it to its default port name.

When you reset a port name to its default, any existing power associations are removed and, if the port is a part of a port group, it is removed from the group.

Port Type

Port type includes:

- DCIM - Dominion CIM
- TierDevice - Tiered device
- Not Available - No CIM connected
- DVM-DP - Display Port CIM
- DVM-HDMI - HDMI CIM
- DVM-DVI - DVI CIM
- PowerStrip (rack PDU) - Power strip connected
- VM - D2CIM - VUSB CIM
- Dual - VM - D2CIM-DVUSB CIM
- Blade Chassis - Blade chassis and the blades associated with that chassis (displayed in a hierarchical order)
- KVM Switch - Generic KVM Switch connection
- PCIM - Paragon CIM

Configuring Standard Target Servers

► **To name the target servers:**

1. Connect all of the target servers if you have not already done so. See ***Step 3: Connect the Equipment*** (see "***Step 3: Connecting the Equipment***" on page 36) for a description of connecting the equipment.
2. Choose Device Settings > Port Configuration. The Port Configuration page opens.
3. Click the Port Name of the target server you want to rename. The Port Page opens.
4. Select Standard KVM Port as the subtype for the port.
5. Assign a name to identify the server connected to that port. The name can be up to 32 characters, and alphanumeric and special characters are allowed.

6. Click OK.

Home > Device Settings > Port Configuration > Port

Port 1

Type: DVM-HDMI

Sub Type:

☒ Standard KVM Port
☐ Blade Chassis
☐ KVM Switch

Name:

HDMI Target

Power Association

Power Strip Name	Outlet Name
None	---
None	---
None	---
None	---

Configuring KVM Switches

The KX III also supports use of hot key sequences to switch between targets on a KVM switch. KVM switching is supported by blade chassis and in tiered configurations.

Important: For user groups to see the KVM switch that you create, you must first create the switch and then create the group. If an existing user group needs to see the KVM switch you are creating, you must recreate the user group.

► To configure KVM switches:

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.
2. Click the Port Name of the target server you want to rename. The Port Page opens.
3. Select KVM Switch.
4. Select the KVM Switch Model.

Note: Only one switch will appear in the drop-down.

5. Select the KVM Switch Hot Key Sequence.
6. Enter the Maximum Number of Target Ports (2-32).

7. In the KVM Switch Name field, enter the name you want to use to refer to this port connection.

Home > Device Settings > Port Configuration > Port

Port 1

Type: DVM-HDMI

Sub Type: ☐ Standard KVM Port ☐ Blade Chassis ☒ KVM Switch

▼ KVM Switch Port Configuration

KVM Switch Model: Generic Analog KVM Switch

KVM Switch Hot Key Sequence: NumLock + NumLock + SlotNumber

Maximum Number of Target Ports (2-32): 32

KVM Switch Name: KVM_Switch_Port1

8. Activate the targets that the KVM switch hot key sequence will be applied to.
- Indicate that the KVM switch ports have targets attached by selecting 'Active' for each of the ports. Use Select All and Deselect All to select and deselect the Active checkboxes accordingly.
- Change the port names as need.

Select All Deselect All

Active	Target 1	Active	Target 2
☒	KVM_Switch_Port1_Target1	☐	KVM_Switch_Port1_Target2
☒	KVM_Switch_Port1_Target3	☐	KVM_Switch_Port1_Target4
☐	KVM_Switch_Port1_Target5	☒	KVM_Switch_Port1_Target6
☐	KVM_Switch_Port1_Target7	☐	KVM_Switch_Port1_Target8

9. In the KVM Managed Links section of the page, you are able to configure the connection to a web browser interface, if one is available.
 - a. Select Active to activate the link once it is entered.
 Leave the checkbox deselected to keep the link inactive.
 You can enter information into the link fields and save without activating the links.
 Once Active is selected, the URL field is required.
 - b. URL Name - Enter the URL to the interface.
 - c. Username - Enter the username used to access the interface.
 - d. Password - Enter the password used to access the interface.

- e. Username Field - Enter the username parameter that will be used in the URL. For example *username=admin*, where *username* is the username field.
- f. Password Field - Enter the password parameter that will be used in the URL. For example *password=raritan*, where *password* is the password field.

10. Click OK.

► **To change the active status/deactivate a KVM switch port or URL:**

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.
2. Click the Port Name of the target server you want to deactivate. The Port Page opens.
3. Deselect the Active checkbox next to the KVM switch target port or URL to deactivate them.
4. Click OK.

Configuring CIM Ports

The KX III supports the use of standard and virtual media CIMs to connect a server to the KX III.

► **To access a CIM to configure:**

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.
2. Click the Port Name of the target server you want to rename. The Port Page opens.
3. Next -

- **Configure the CIM Settings** (on page 103)
- **Configure the CIM Power Associations** (on page 103)
- **Configure the CIM Target Settings** (on page 103)
- **Apply Selected Profiles to Other CIMs** (on page 104)
- **Apply a Native Display Resolution to Other CIMs** (on page 105)

Configure the CIM Settings

1. Select Standard KVM Port as the subtype for the port.
2. Assign a name to identify the server connected to that port. The name can be up to 32 characters, and alphanumeric and special characters are allowed.

Port 1

Type: DVM-DVI

Sub Type: ☒ Standard KVM Port
☐ Blade Chassis
☐ KVM Switch

Name:

Configure the CIM Power Associations

1. In the Power Association section, associate a power strip with the port, if needed.

Power Association

Power Strip Name	Outlet Name
None ▼	---
None ▼	---
None ▼	---
None ▼	---

Configure the CIM Target Settings

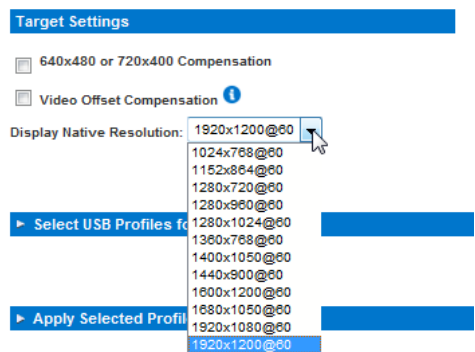
1. In the Target Settings section, select "640x480 or 720x400 Compensation" if you are experiencing display issues when the target is using this resolution.
2. In the Target Settings section, select "Video Offset Compensation" if the video appears off center on your target.

Target Settings

☐ 640x480 or 720x400 Compensation

☐ Video Offset Compensation ⓘ

3. For digital CIMs, to set the target's video resolution to match your monitor's native display resolution, select the resolution from the Display Native Resolution drop-down.

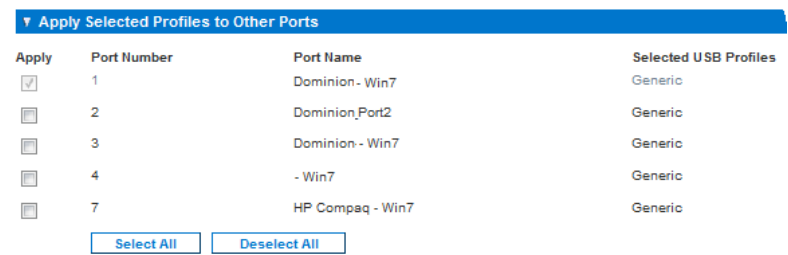


For a complete list of supported video resolutions from the remote console, see *KX III Supported Local Port DVI Resolutions* (on page 420)

4. If you are using an HDMI CIM, some operating system/video card combinations may offer a limited range of RGB values. Improve the colors by selecting the DVI Compatibility Mode checkbox under the Target Settings section.

Apply Selected Profiles to Other CIMs

1. Apply the profile to other CIMs by selecting them from the list in the Apply Selected Profiles to Other Ports section of the Port Configuration page.



Apply a Native Display Resolution to Other CIMs

1. Apply the native display resolution to the CIM or to other CIMs of the same type by selecting the ports other CIMs are connected to from the list in the Apply Native Resolutions to Other Ports section of the Port Configuration page.

▼ Apply Native Resolution to Other Ports			
Apply	Port Number	Port Name	Native Resolution
☒	1	Dominion - Win7	1600x1200@60
Select All Deselect All			

Configuring Rack PDU (Power Strip) Targets

KX III allows you to connect rack PDUs (power strips) to KX III ports. KX III rack PDU configuration is done from the KX III Port Configuration page.

Note: Raritan recommends no more than eight (8) rack PDUs (power strips) be connected to a KX III at once since performance may be affected.

Connecting a Rack PDU

Raritan PX series rack PDUs (power strips) are connected to the Dominion device using the D2CIM-PWR CIM.

► To connect the rack PDU:

1. Connect the male RJ-45 of the D2CIM-PWR to the following female RJ-45 connector of the rack PDU.
 - PX1 series: RJ-45 "SERIAL" port
 - PX2, PX3 or PX3TS series: RJ-45 "FEATURE" port
2. Connect the female RJ-45 connector of the D2CIM-PWR to any of the available female system port connectors on the KX III using a straight through Cat5 cable.
3. Attach an AC power cord to the target server and an available rack PDU outlet.
4. Connect the rack PDU to an AC power source.

5. Power on the device.

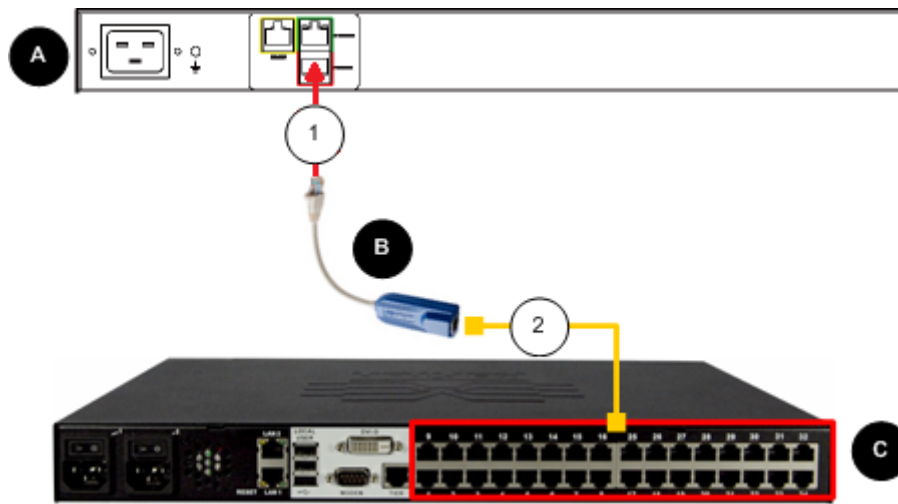


Diagram key

A	PX rack PDU with serial port
B	D2CIM-PWR
C	KX III
1	D2CIM-PWR to rack PDU serial port connection
2	D2CIM-PWR to KX III target device port via Cat5 cable

Naming the Rack PDU (Port Page for Power Strips)

Note: PX rack PDUs (power strips) can be named in the PX as well as in the KX III.

Once a Raritan remote rack PDU is connected to the KX III, it will appear on the Port Configuration page. Click on the power port name on that page to access it. The Type and the Name fields are prepopulated.

Note: The (CIM) Type cannot be changed.

The following information is displayed for each outlet on the rack PDU: [Outlet] Number, Name, and Port Association.

Use this page to name the rack PDU and its outlets. Names can be up to 32 alphanumeric characters and can include special characters.

Note: When a rack PDU is associated with a target server (port), the outlet name is replaced by the target server name, even if you assigned another name to the outlet.

► **To name the rack PDU and outlets:**

Note: CommandCenter Secure Gateway does not recognize rack PDU names containing spaces.

1. Enter the Name of the rack PDU (if needed).
2. Change the [Outlet] Name if desired. (Outlet names default to the outlet #.)

3. Click OK.

Home > Device Settings > Port Configuration > Port

Port 17

Type:
PowerStrip

Name:

Outlets

Number	Name	Port Association
1	Dominion-Port1(1)	Dominion- Port7
2	Outlet 2	
3	Outlet 3	
4	Outlet 4	
5	Outlet 5	
6	Outlet 6	
7	Outlet 7	
8	Outlet 8	

Associating Outlets with Target Devices

The Port page opens when you click on a port on the Port Configuration page.

If an outlet is connected to the same server that the port is connected to, a power association can be made with the target device.

A server can have up to four power plugs and you can associate a different rack PDU (power strip) with each. From this page, you can define those associations so that you can power on, power off, and power cycle the server from the Port Access page.

To use this feature, you will need:

- Raritan remote rack PDU(s)
- Power CIMs (D2CIM-PWR)

Make a Power Association

► **To make power associations (associate rack PDU outlets to KVM target servers):**

Note: When a rack PDU is associated to a target server (port), the outlet name is replaced by the target server name (even if you assigned another name to the outlet).

1. On the Port Configuration page, select the target server you are associating the PDU with.
2. Choose the rack PDU from the Power Strip Name drop-down list.
3. For that rack PDU, choose the outlet from the Outlet Name drop-down list.
4. Repeat steps 1 and 2 for all desired power associations.
5. Click OK. A confirmation message is displayed.

Remove a Power Association

When disconnecting target servers and/or rack PDUs from the device, all power associations should first be deleted. When a target has been associated with a rack PDU and the target is removed from the device, the power association remains. When this occurs, you are not able to access the Port Configuration for that disconnected target server in Device Settings so that the power association can be properly remove.

► **To remove a rack PDU association:**

1. Select the appropriate rack PDU from the Power Strip Name drop-down list.
2. For that rack PDU, select the appropriate outlet from the Outlet Name drop-down list.
3. From the Outlet Name drop-down list, select None.

4. Click OK. That rack PDU/outlet association is removed and a confirmation message is displayed.
- **To remove a rack PDU association if the rack PDU has been removed from the target:**
1. Click Device Settings > Port Configuration and then click on the active target.
 2. Associate the active target to the disconnected power port. This will break the disconnected target's power association.
 3. Finally, associate the active target to the correct power port.

Configuring Blade Chassis

In addition to standard servers and rack PDUs (power strips), you can control blade chassis that are plugged into the KX III port. Up to eight blade chassis can be managed at a given time.

If the blade chassis type is supported, it is automatically detected once it is connected.

When a blade chassis is detected, a default name is assigned to it and it is displayed on the Port Access page along with standard target servers and rack PDUs.

If the type is not supported, the blade must be configured manually. The blade chassis must be configured as a blade chassis subtype.

For more information on how blades are displayed, see *Port Access Page (Remote Console Display)* (on page 21).

Generic Blade Chassis Configuration

The Generic Blade Chassis' selection provides only a manual configuration mode of operation.

See *Supported Blade Chassis Models* (on page 131), *Supported CIMs for Blade Chassis* (on page 131), and *Required and Recommended Blade Chassis Configurations* (on page 134) for important, additional information when configuring the blade chassis.

See *Dell Chassis Cable Lengths and Video Resolutions* (on page 428) for information on cable lengths and video resolutions when using Dell® chassis with the KX III.

- **To configure a generic blade chassis:**
1. Connect the blade chassis to the KX III.
 2. Select Device Settings > Port Configuration to open the Port Configuration page.
 3. On the Port Configuration page, click on the name of the blade chassis you want to configure. The Port page will open.

4. Select the Blade Chassis radio button.
The page will then display the necessary fields to configure a blade chassis.
5. Select Generic from the Blade Server Chassis Model drop-down.

Home > Device Settings > Port Configuration > Port

Port 3

Type: DVM-DVI Sub Type: ☐ Standard KVM Port ☒ Blade Chassis ☐ KVM Switch

▼ Blade Server Chassis Port Configuration

Blade Server Chassis Model: Generic

Switch Hot Key Sequence: NumLock + NumLock + SlotNumber Maximum Number of Slots (2-16): 16

Administrative Module Primary IP Address/Host Name:
 Port Number: 22

Username:
 Password:

6. Configure the blade chassis as applicable.
 - Switch Hot Key Sequence - Define the hot key sequence that will be used to switch from KVM to the blade chassis.
The Switch Hot Key Sequence must match the sequence used by the KVM module in the blade chassis.

Home > Device Settings > Port Configuration > Port

Port 3

Type: DVM-DVI Sub Type: ☐ Standard KVM Port ☒ Blade Chassis ☐ KVM Switch

▼ Blade Server Chassis Port Configuration

Blade Server Chassis Model: Generic

Switch Hot Key Sequence: NumLock + NumLock + SlotNumber Maximum Number of Slots (2-16): 16

Administrative Module Primary IP Address/Host Name:
 Port Number: 22

Username:
 Password:

- Maximum Number of Slots - Enter the default maximum number of slots available on the blade chassis.
- Administrative Module Primary IP Address/Host Name - Not applicable.
- Username - Not applicable.
- Password - Not applicable.

- Port Number - The default port number for the blade chassis is 22. Not applicable.
7. Change the blade chassis name, if needed.
 8. Check the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox.
- If needed, change the blade server names.

9. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available.

Click the Blade Chassis Managed Links icon to expand the section on the page.

► Blade Chassis Managed Links

The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

- Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.
- URL - Enter the URL to the interface. **Required**
- Username - Enter the username used to access the interface. **Optional**

- Password - Enter the password used to access the interface.
Optional

▼ Blade Chassis Managed Links

Administrative Module

Active ☐ URL

Username Password

Username Field Password Field

Other Useful URLs

Active ☐ URL Name

Blade_Chassis_Port3_URL_B

URL

Username Password

Username Field Password Field

URL Name

☐ Blade_Chassis_Port3_URL_C

URL

Username Password

Username Field Password Field

Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

- The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries.
Enter the field names for the username and password fields used on web application's login page. For example, the web application's login page may use fields named "userID" and "userpassword".
You can view the HTML source of the login screen in your browser to find the field *names*. Note that these are not the field labels.

- See *Tips for Adding a Web Browser Interface* (on page 128) for tips on adding a web browser interface.

Administrative Module

Active URL

Username Password

Username Field Password Field

Other Useful URLs

Active URL Name

Blade_Chassis_Port3_URL_B

URL

Username Password

Username Field Password Field

URL Name

- In the Target Settings section, select "640x480 or 720x400 Compensation" if you are experiencing display issues when the target is using this resolution.
- In the Target Settings section, select "Video Offset Compensation" if the video appears off center on your target.

Target Settings

☐ 640x480 or 720x400 Compensation

☒ Video Offset Compensation ⓘ

- For digital CIMs, to set the target's video resolution to match your monitor's native display resolution, select the resolution from the Display Native Resolution drop-down.

Target Settings

☐ 640x480 or 720x400 Compensation

☒ Video Offset Compensation ⓘ

Display Native Resolution: 1920x1200@60

1024x768@60

1152x864@60

1280x720@60

1280x960@60

1280x1024@60

1360x768@60

1400x1050@60

1440x900@60

1600x1200@60

1680x1050@60

1920x1080@60

1920x1200@60

► Select USB Profiles for

► Apply Selected Profile

For a complete list of supported video resolutions from the remote console, see *KX III Supported Local Port DVI Resolutions* (on page 420)

- USB profile information does not apply to a generic configuration.

14. Select 'Use international keyboard for scan code set 3' if connecting to the target with a DCIM-PS2 and require the use of scan code set 3 with an international keyboard.
15. Click OK to save the configuration.

Blade Chassis Configuration Options

With the exception of HP and Cisco® UCS blade chassis, the generic, IBM® and Dell® blade chassis are configured on the Port page.

The port connected to the blade chassis must be configured with the blade chassis model.

The specific information you are able to configure for a blade server will depend on the brand of blade server you are working with. For specific information on each of these supported blade chassis, see their corresponding topics in this section of the help.

Dell

- Dell PowerEdge® 1855, 1955 and M1000e
Dell PowerEdge 1855/1955 blades also provide the ability to connect from each individual blade to a port on the Dominion appliance. When connected in that manner, they can also be grouped to create blade server groups.

IBM

- IBM BladeCenter® Models E and H

Generic

- A Generic option allows you to configure a blade chassis that is not a Dell PowerEdge® 1855, 1955 and M1000e, IBM BladeCenter® Models E and H, HP BladeSystem c3000 and c7000, or Cisco UCS blade server.

HP

- HP BladeSystem c3000 and c7000, and Cisco UCS blade servers are supported via individual connections from the Dominion appliance to each blade.

The ports are 'grouped' together into a chassis representation using the Port Group Management feature.

Manual and Auto-Discovery Blade Chassis Configuration

Two modes of operation are provided for blade chassis: manual configuration and auto-discovery, depending on the blade chassis capabilities.

Configure the mode by selecting Device Services > Port Configuration to open the Port page. Options are available in the "Blade Server Chassis Port Configuration" section of the page.

[Home](#) > [Device Settings](#) > [Port Configuration](#) > [Port](#)

Port 3

Type: DVM-DVI

Sub Type:

☐ Standard KVM Port
☒ Blade Chassis
☐ KVM Switch

Blade Server Chassis Port Configuration

Blade Server Chassis Model

Generic

Switch Hot Key Sequence

NumLock + NumLock + SlotNumber

Maximum Number of Slots (2-16)

16

Administrative Module Primary IP Address/Host Name

Port Number

22

Username

Password

☐ Blade Auto-Discovery

Discover Blades in Chassis Now

Blade Chassis Name

Blade_Chassis_Port3

If a blade chassis is configured for auto-discovery, the Dominion appliance tracks and updates the following:

- When a new blade server is added to the chassis.
- When an existing blade server is removed from the chassis.

Note: In the case of IBM Blade Center Models E and H, the KX III only supports auto-discovery for AMM[1] as the acting primary management module.

Select the "Blade Auto-Discovery" checkbox to enable auto-discovery. To locate a blade at this time, click the "Discover Blades in Chassis Now" button.

Hot Key Sequences to Access Blade Chassis

The use of hot key sequences to switch KVM access to a blade chassis is supported.

For blade chassis that allow users to select a hot key sequence, those options will be provided on the Port Configuration page.

For example, the Dell PowerEdge M1000e allows users to select from a list of default hot key sequences.

The hot key sequences specific to the M1000e are listed in the "Switch Hot Key Sequence" drop-down when the M1000e is selected.

▼ Blade Server Chassis Port Configuration

Blade Server Chassis Model
Dell PowerEdge M1000e

Switch Hot Key Sequence
PrintScreen + SlotNumber
PrintScreen + SlotNumber
Ctrl + Ctrl + SlotNumber
Shift + Shift + SlotNumber
Alt + Alt + SlotNumber

Maximum Number of Slots (2-16)
16

Port Number
22

Password

For blade chassis that come with predefined hot key sequences, those sequences will be prepopulated on the Port Configuration page once the blade chassis is selected.

For example, the default hot key sequence to switch KVM access to an IBM BladeCenter H is NumLock + NumLock + SlotNumber.

This hot key sequence is applied by default when IBM BladeCenter H is selected during the configuration.

▼ Blade Server Chassis Port Configuration

Blade Server Chassis Model
IBM BladeCenter H

Switch Hot Key Sequence
NumLock + NumLock + SlotNumber

Maximum Number of Slots (2-16)
14

Administrative Module Primary IP Address/Host Name

Port Number
22

Username

Password

See your blade chassis documentation for hot key sequence information.

Link to a Blade Chassis Interface - Blade Chassis Managed Links

You are able to configure the connection to a blade chassis web browser interface if one is available.

Configure links when adding a blade by selecting Device Services > Port Configuration, and entering the link information in the Blade Chassis Managed Links section of the page.

At the chassis level, up to four links can be defined.

The first link is reserved for connection to the blade chassis administrative module GUI.

For example, this link may be used by technical support to quickly verify a chassis configuration.

▼ Blade Chassis Managed Links

Administrative Module

☐

Active URL

Username

Username Field

Password

Password Field

Other Useful URLs

☐

URL Name

Blade_Chassis_Port3_URL_B

URL

Username

Username Field

Password

Password Field

☐

URL Name

Blade_Chassis_Port3_URL_C

URL

Username

Username Field

Password

Password Field

Managing Blade Chassis

Blade chassis can be managed from the Virtual KVM Client (VKC), Active KVM Client (AKC), and CC-SG.

Managing blade servers via VKC and AKC is the same as managing standard target servers.

See *Virtual KVM Client (VKC) Help* (see "Virtual KVM Client (VKC and VKCs) Help" on page 256), *Active KVM Client (AKC) Help* (on page 301) and the **CC-SG Administrators Guide** for more information.

Note: Any changes made to the blade chassis configuration will be propagated to these client applications.

Important: When the CIM connecting the blade chassis to the Dominion appliance is powered down or disconnected from the Dominion device, all established connections to the blade chassis are dropped. When the CIM is reconnected or powered up, you need to re-establish the connection(s).

Dell Blade Chassis Configuration

See *Supported Blade Chassis Models* (on page 131), *Supported CIMs for Blade Chassis* (on page 131), and *Required and Recommended Blade Chassis Configurations* (on page 134) for important, additional information when configuring the blade chassis.

See *Dell Chassis Cable Lengths and Video Resolutions* (on page 428) for information on cable lengths and video resolutions when using Dell® chassis with the KX III.

► **To add a blade chassis:**

1. Connect the blade chassis to the KX III.
2. Select Device Settings > Port Configuration to open the Port Configuration page.
3. On the Port Configuration page, click on the name of the blade chassis you want to configure. The Port page will open.
4. Select the Blade Chassis radio button. The page will then display the necessary fields to configure a blade chassis.
5. Select the Dell blade chassis model from the Blade Server Chassis Model drop-down.

► **To configure a Dell PowerEdge M1000e:**

1. If you selected Dell PowerEdge™ M1000e, auto-discovery is available. Configure the blade chassis as applicable. Prior to configuring a blade chassis that can be auto-discovered, it must be configured to enable SSH connections on the designated port number (see **Device Services** (on page 143)). Additionally, a user account with the corresponding authentication credentials must be previously created on the blade chassis.
 - a. Switch Hot Key Sequence - Select the hot key sequence that will be used to switch from KVM to the blade server. The Switch Hot Key Sequence must match the sequence used by the KVM module in the blade chassis.
 - b. Maximum Number of Slots - The default maximum number of slots available on the blade chassis is automatically entered.
 - c. Administrative Module Primary IP Address/Host Name - Enter the primary IP address for the blade chassis. **Required for auto-discovery mode**
 - d. Port Number - The default port number for the blade chassis is 22. Change the port number if applicable. **Required for auto-discovery mode**
 - e. Username - Enter the username used to access the blade chassis. **Required for auto-discovery mode**
 - f. Password - Enter the password used to access the blade chassis. **Required for auto-discovery mode**
2. If you want the KX III to auto-discover the chassis blades, select the Blade Auto-Discovery checkbox and then click Discover Blades on Chassis Now. Once the blades are discovered, they will be displayed on the page.
3. Change the blade chassis name if needed. If the chassis is already named, that information automatically populates this field. If it is not already named, the KX III assigns the chassis a name. The default naming convention for the blade chassis by the KX III is Blade_Chassis_Port#.
4. If operating in Manual mode, indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox. If needed, change the blade server names
If operating in Auto-discovery mode, the Installed box will display the slots containing blades during discovery.
5. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available.

Click the Blade Chassis Managed Links icon to expand the section on the page.

► Blade Chassis Managed Links

The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

- a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.
 - b. URL - Enter the URL to the interface. See **Blade Chassis Sample URL Formats** (on page 136) for sample configurations for the Dell M1000e.
 - c. Username - Enter the username used to access the interface.
 - d. Password - Enter the password used to access the interface.
-

Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

- e. The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries.
 Enter the field names for the username and password fields used on web application's login page. For example, the web application's login page may use fields named "userID" and "userpassword".
 You can view the HTML source of the login screen in your browser to find the field *names*. Note that these are not the field labels.
6. See **Tips for Adding a Web Browser Interface** (on page 128) for tips on adding a web browser interface.
7. USB profiles do not apply to Dell chassis.
8. In the Target Settings section, select 720x400 Compensation if you are experiencing display issues when the target is using this resolution.
9. Select 'Use international keyboard for scan code set 3' if connecting to the target with a DCIM-PS2 and require the use of scan code set 3 with an international keyboard.

10. Select the CIMs native, display resolution from the Display Native Resolution drop-down. This is the preferred resolution and timing mode of the digital CIM. Once a resolution is selected, it is applied to the CIM.

If no selection is made, the default 1024x1280@60Hz resolution is used.

11. Click OK to save the configuration.

► **To configure a Dell PowerEdge 1855/1955:**

1. If you selected Dell 1855/1955, auto-discovery *is not available*. Configure the blade chassis as applicable.
 - a. Switch Hot Key Sequence - Select the hot key sequence that will be used to switch from KVM to the blade server. For Dell 1855/1955 models, KX III blocks all existing hot key sequences. If you apply a Generic configuration to the Dell 1855, only one existing hot key is blocked.
 - b. Maximum Number of Slots - The default maximum number of slots available on the blade chassis is automatically entered.
 - c. Administrative Module Primary IP Address/Host Name - Not applicable.
 - d. Port Number - The default port number for the blade chassis is 22. Not applicable.
 - e. Username - Not applicable.
 - f. Password - Not applicable.
2. Change the blade chassis name if needed.
3. Indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox. If needed, change the blade server names.
4. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available.

Click the Blade Chassis Managed Links icon to expand the section on the page.

► **Blade Chassis Managed Links**

The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

- a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.
- b. URL - Enter the URL to the interface. See Blade Chassis Sample URL Formats for sample configurations for the Dell PowerEdge 1855/1955.
- c. Username - Enter the username used to access the interface.
- d. Password - Enter the password used to access the interface.

Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

- e. The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries.

Enter the field names for the username and password fields used on web application's login page. For example, the web application's login page may use fields named "userID" and "userpassword".

You can view the HTML source of the login screen in your browser to find the field *names*. Note that these are not the field labels.
 - f. See ***Tips for Adding a Web Browser Interface*** (on page 128) for tips on adding a web browser interface.
- 5. USB profiles do not apply to Dell chassis.
 - 6. Click OK to save the configuration.

IBM Blade Chassis Configuration

See ***Supported Blade Chassis Models*** (on page 131), ***Supported CIMs for Blade Chassis*** (on page 131), and ***Required and Recommended Blade Chassis Configurations*** (on page 134) for important, additional information when configuring the blade chassis.

See ***Dell Chassis Cable Lengths and Video Resolutions*** (on page 428) for information on cable lengths and video resolutions when using Dell® chassis with the KX III.

► **To add a blade chassis:**

- 1. Connect the blade chassis to the KX III.
- 2. Select Device Settings > Port Configuration to open the Port Configuration page.

3. On the Port Configuration page, click on the name of the blade chassis you want to configure. The Port page will open.
4. Select the Blade Chassis radio button. The page will then display the necessary fields to configure a blade chassis.
5. Select the IBM® blade chassis model from the Blade Server Chassis Model drop-down.

► **To configure a IBM BladeCenter H and E:**

1. If you selected IBM BladeCenter® H or E, auto-discovery is available. Configure the blade chassis as applicable. Prior to configuring a blade chassis that can be auto-discovered, it must be configured to enable SSH connections on the designated port number (see *Device Services* (on page 143)). Additionally, a user account with the corresponding authentication credentials must be previously created on the blade chassis. The KX III only supports auto-discovery for AMM[1].
 - a. Switch Hot Key Sequence - Predefined.
 - b. Maximum Number of Slots - The default maximum number of slots available on the blade chassis is automatically entered.
 - c. Administrative Module Primary IP Address/Host Name - Enter the primary IP address for the blade chassis. **Required for auto-discovery mode**
 - d. Port Number - The default port number for the blade chassis is 22. Change the port number if applicable. **Required for auto-discovery mode**
 - e. Username - Enter the username used to access the blade chassis. **Required for auto-discovery mode**
 - f. Password - Enter the password used to access the blade chassis. **Required for auto-discovery mode**
2. If you want the KX III to auto-discover the chassis blades, select the Blade Auto-Discovery checkbox and then click Discover Blades on Chassis Now. Once the blades are discovered, they will be displayed on the page.
3. Change the blade chassis name if needed. If the chassis is already named, that information automatically populates this field. If it is not already named, the KX III assigns the chassis a name. The default naming convention for the blade chassis by the KX III is Blade_Chassis_Port#.
4. If operating in Manual mode, indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox. If needed, change the blade server names

If operating in Auto-discovery mode, the Installed box will display the slots containing blades during discovery.

5. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available.

Click the Blade Chassis Managed Links icon to expand the section on the page.

► Blade Chassis Managed Links

The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

- a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.
- b. URL - Enter the URL to the interface. See **Blade Chassis Sample URL Formats** (on page 136) for sample configurations for the IBM BladeCenter.
- c. Username - Enter the username used to access the interface.
- d. Password - Enter the password used to access the interface.

Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

- e. The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries.

Enter the field names for the username and password fields used on web application's login page. For example, the web application's login page may use fields named "userID" and "userpassword".

You can view the HTML source of the login screen in your browser to find the field *names*. Note that these are not the field labels.
- f. See **Tips for Adding a Web Browser Interface** (on page 128) for tips on adding a web browser interface.

6. If applicable, define the USB profile for the blade chassis or select an existing USB profile. Click the USB Profiles Select USB Profiles for Port icon **► Select USB Profiles for Port** or the Apply Select Profiles to Other Ports icon **► Apply Selected Profiles to Other Ports** to expand these sections of the page. See *Configuring USB Profiles (Port Page)* (on page 137).
7. Click OK to save the configuration.

► To configure a IBM BladeCenter (Other):

1. If you selected IBM BladeCenter (Other), auto-discovery *is not* available. Configure the blade chassis as applicable.
 - a. Switch Hot Key Sequence - Select the hot key sequence that will be used to switch from KVM to the blade server.
 - b. Administrative Module Primary IP Address/Host Name - Enter the primary IP address for the blade chassis. Not applicable.
 - c. Maximum Number of Slots - Enter the default maximum number of slots available on the blade chassis.
 - d. Port Number - The default port number for the blade chassis is 22. Not applicable.
 - e. Username - Not applicable.
 - f. Password - Not applicable.
2. Change the blade chassis name if needed.
3. Indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox. If needed, change the blade server names. If it is not already named, the KX III assigns a name to the blade server. The default blade server naming convention is Blade_Chassis_Port#_Slot#.
4. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available.

Click the Blade Chassis Managed Links icon to expand the section on the page.

► Blade Chassis Managed Links

The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

- a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.
- b. URL - Enter the URL to the interface. See **Blade Chassis Sample URL Formats** (on page 136) for sample configurations for the IBM BladeCenter.
- c. Username - Enter the username used to access the interface.
- d. Password - Enter the password used to access the interface.

Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

- e. The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries.

Enter the field names for the username and password fields used on web application's login page. For example, the web application's login page may use fields named "userID" and "userpassword".

You can view the HTML source of the login screen in your browser to find the field *names*. Note that these are not the field labels.
- f. See **Tips for Adding a Web Browser Interface** (on page 128) for tips on adding a web browser interface.

- 5. USB profiles are not used by IBM (Other) configurations.
- 6. In the Target Settings section, select 720x400 Compensation if you are experiencing display issues when the target is using this resolution.
- 7. Select 'Use international keyboard for scan code set 3' if connecting to the target with a DCIM-PS2 and require the use of scan code set 3 with an international keyboard.

Select the CIMs native, display resolution from the Display Native Resolution drop-down. This is the preferred resolution and timing mode of the digital CIM. Once a resolution is selected, it is applied to the CIM.

- 1. If no selection is made, the default 1024x1280@60Hz resolution is used.
- 2. Click OK to save the configuration.

Tips for Adding a Web Browser Interface

You can add a Web Browser Interface to create a connection to a device with an embedded web server. A Web Browser interface can also be used to connect to any web application, such as the web application associated with an RSA, DRAC or ILO Processor card.

You must have DNS configured or URLs will not resolve. You do not need to have DNS configured for IP addresses.

► To add a web browser interface:

1. The default name for a Web Browser Interface is provided. If needed, change the name in the Name field.
2. Enter the URL or domain name for the web application in the URL field. You must enter the URL at which the web application expects to read the username and password.

Follow these examples for correct formats:

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

3. Enter the username and password that will allow access to this interface. **Optional**
4. If username and password were entered, in the Username Field and Password Field, type the field names for the username and password fields that are used in the login screen for the web application. You must view the HTML source of the login screen to find the field names, not the field labels.

Tip for locating field names:

- In the HTML source code for the login page of the web application, search for the field's label, such as Username and Password.
- When you find the field label, look in the adjacent code for a tag that looks like this: `name="user"`. The word in quotes is the field name.

HP and Cisco UCS Blade Chassis Configuration (Port Group Management)

The KX III supports the aggregation of ports connected to certain types of blades into a group representing the blade chassis. Specifically, Cisco® UCS, HP® BladeServer blades and Dell® PowerEdge™ 1855/1955 blades when the Dell PowerEdge 1855/1955 is connected from each individual blade to a port on the KX III.

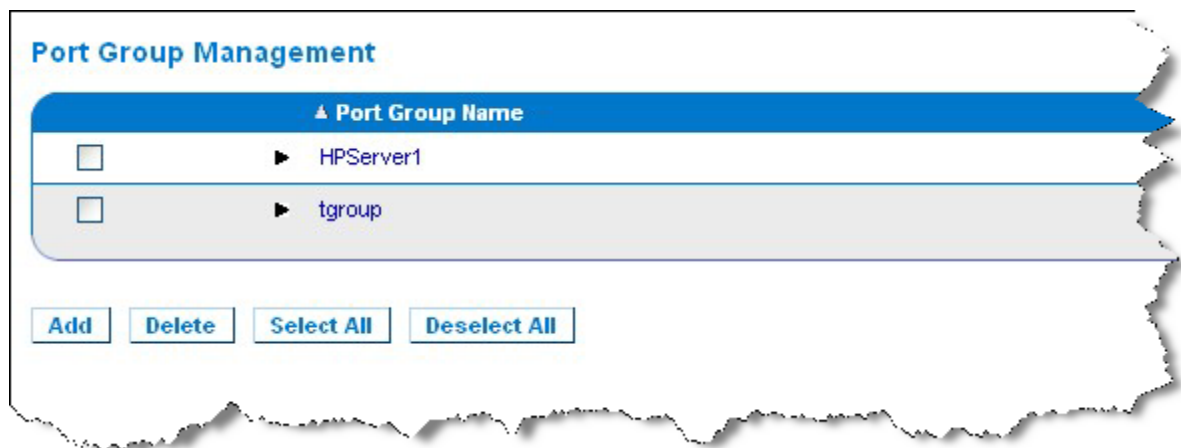
The chassis is identified by a Port Group Name and the group is designated as a Blade Server Group on the Port Group Management page. Port Groups consist solely of ports configured as standard KVM ports, not ports configured as blade chassis. A port may only be a member of a single group.

Ports connected to integrated KVM modules in a blade chassis are configured as blade chassis subtypes. These ports are eligible to be included in port groups.

When KX III ports are connected to integrated KVM modules in a blade chassis and not to individual blades, the ports are configured as blade chassis subtypes. These ports are not eligible to be included in port groups and will not appear in the Select Port for Group, Available list.

If a standard KVM port has been included in a port group, and then is subsequently repurposed for use as a blade chassis subtype, it must first be removed from the port group.

Port Groups are restored using the Backup and Restore option.



► **To add a port group:**

1. Click Device Settings > Port Group Management to open the Port Group Management page.
2. Click Add to open the Port Group page.
3. Enter a Port Group Name. The port group name is not case sensitive and can contain up to 32 characters.

4. Select the Blade Server Group checkbox.

If you want to designate that these ports are attached to blades housed in a blade chassis (for example, HP c3000 or Dell PowerEdge 1855), select the Blade Server Group checkbox.

Note: This is especially important to CC-SG users who want HP blades to be organized on a chassis basis, although each blade has its own connection to a port on the KX III.

5. Click on a port in the Available box in the Select Ports for Group section. Click Add to add the port to the group. The port will be moved to the Selected box.
6. Click OK to add the port group.

Home > Device Settings > Port Group Management > Port Group

Port Group

Port Group Name
HPServer1

☒ Blade Server Group
☐ Dual Video Port Group
☐ Port Group

Select Ports for Group

Available:
KX 192.168.60.109 - Dell M1000e

Add >
< Remove

Selected:

OK Cancel

► **To edit port group information:**

1. On the Port Group Management page, click on the link of the port group you want to edit. The Port Group page opens.
2. Edit the information as needed.
3. Click OK to save the changes.

► **To delete a port group:**

1. Click on the Port Group Management page, select the checkbox of the port group you want to delete.
2. Click Delete.
3. Click OK on the warning message.

Supported Blade Chassis Models

This table contains the blade chassis models that are supported by the KX III and the corresponding profiles that should be selected per chassis model when configuring them in the KX III application. A list of these models can be selected on the Port Configuration page from the Blade Server Chassis Model drop-down, which appears when the Blade Chassis radio button is selected. For details on how to configure each blade chassis model, see their corresponding topics in this section of the help.

Blade chassis model	KX III Profile
Cisco® UCS	Configure using Port Group Management functions. See <i>HP and Cisco UCS Blade Chassis Configuration (Port Group Management)</i> (on page 129)
Dell® PowerEdge™ 1855/1955	Dell PowerEdge 1855/1955
Dell PowerEdge M1000e	Dell PowerEdge M1000e
IBM® BladeCenter® S	IBM (Other)
IBM BladeCenter H	IBM BladeCenter H
IBM BladeCenter T	IBM (Other)
IBM BladeCenter HT	IBM (Other)
IBM BladeCenter E	IBM BladeCenter E
HP®	Configure using Port Group Management functions. See <i>HP and Cisco UCS Blade Chassis Configuration (Port Group Management)</i> (on page 129)

Supported CIMs for Blade Chassis

The following CIMs are supported for blade chassis being managed through the KX III:

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

Following is a table containing supported CIMs for each blade chassis model that the KX III supports.

Blade chassis	Connection method	Recommended CIM(s)
Generic	If a D2CIM-VUSB or D2CIM-DVUSB is used when connecting to a blade-chassis configured as Generic, you will be able to select the USB profiles from the Port Configuration page and the client's USB Profile menu. However, virtual media is not supported for generic blade chassis and the Virtual Media menu is disabled on the client.	• DCIM-PS2 • DCIM-USBG2
Cisco® UCS Server Chassis	The Cisco KVM cable (N20-BKVM) enables you to perform server blade administration, configuration, and diagnostic procedures by connecting video and USB devices directly to the server blade. Source: <i>Cisco UCS 5108 Server Chassis Installation Guide</i>	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB
Dell® PowerEdge™ 1855	Includes one of the three KVM modules : • Analog KVM Ethernet switch module (standard) • Digital Access KVM switch module (optional) • KVM switch module (standard on systems sold prior to April, 2005) These switches provide a custom connector that allows two PS/2 and one video device to be connected to the system. Source: <i>Dell PowerEdge 1855 User Guide</i>	• DCIM-PS2
Dell PowerEdge 1955	One of two types of KVM modules may be installed: • Analog KVM switch module • Digital Access KVM switch module Both modules enable you to connect a PS/2-compatible keyboard, mouse and video monitor to the system (using a custom cable provided with the system). Source: <i>Dell PowerEdge 1955 Owner's Manual</i>	• DCIM-PS2
Dell PowerEdge M1000e	The KVM Switch Module (iKVM) is Integrated with this chassis. The iKVM is compatible with the following peripherals:	• DCIM-USBG2

Blade chassis	Connection method	Recommended CIM(s)
	• USB keyboards, USB pointing devices • VGA monitors with DDC support. Source: <i>Dell Chassis Management Controller, Firmware Version 1.0, User Guide</i>	
HP® BladeSystem c3000	The HP c-Class Blade SUV Cable enables you to perform blade chassis administration, configuration, and diagnostic procedures by connecting video and USB devices directly to the server blade. Source: <i>HP ProLiant™ BL480c Server Blade Maintenance and Service Guide</i>	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (for standard KVM port operation without a KVM option)
HP BladeSystem c7000	The HP c-Class Blade SUV Cable enables you to perform server blade administration, configuration, and diagnostic procedures by connecting video and USB devices directly to the server blade. Source: <i>HP ProLiant BL480c Server Blade Maintenance and Service Guide</i>	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (for standard KVM port operation)
IBM® BladeCenter® S	The Advanced Management Module (AMM) provides system management functions and keyboard/video/mouse (KVM) multiplexing for all blade chassis. The AMM connections include: a serial port, video connection, remote management port (Ethernet), and two USB v2.0 ports for a keyboard and mouse. Source: <i>Implementing the IBM BladeCenter S Chassis</i>	• DCIM-USBG2
IBM BladeCenter H	The BladeCenter H chassis ships standard with one Advanced Management Module. Source: <i>IBM BladeCenter Products and Technology</i>	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter E	The current model BladeCenter E chassis (8677-3Rx) ships standard with one Advanced Management Module. Source: <i>IBM BladeCenter Products and Technology</i>	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	The BladeCenter T chassis ships standard with	• DCIM-PS2

Blade chassis	Connection method	Recommended CIM(s)
	one Advanced Management Module. In contrast to the standard BladeCenter chassis, the KVM module and the Management Module in the BladeCenter T chassis are separate components. The front of the Management Module only features the LEDs for displaying status. All Ethernet and KVM connections are fed through to the rear to the LAN and KVM modules. The KVM module is a hot swap module at the rear of the chassis providing two PS/2 connectors for keyboard and mouse, a systems-status panel, and a HD-15 video connector. Source: <i>IBM BladeCenter Products and Technology</i>	
IBM BladeCenter HT	The BladeCenter HT chassis ships standard with one Advanced Management Module. This module provides the ability to manage the chassis as well as providing the local KVM function. Source: <i>IBM BladeCenter Products and Technology</i>	• DCIM-USBG2

Note: In order to support Auto-discovery, IBM BladeCenter Models H and E must use AMM with firmware version BPET36K or later.

Note: In the case of IBM Blade Center Models E and H, the KX III only supports auto-discovery for AMM[1] as the acting primary management module.

Note: Audio is disabled for all KVM switch targets.

Required and Recommended Blade Chassis Configurations

This table contains information on limitations and constraints that apply to configuring blade chassis to work with the KX III. Raritan recommends that all of the information below is followed.

Blade chassis	Required/recommended action
Dell® PowerEdge™ M1000e	▪ Disable the iKVM GUI screensaver. An authorize dialog will appear, preventing iKVM from working correctly, if this is not done. ▪ Exit the iKVM GUI menu before attaching Dell's chassis to a Raritan CIM. iKVM may not work correctly if this is not done. ▪ Configure the iKVM GUI Main menu to select target blades by Slot, not by Name. iKVM may not work correctly if this is not done. ▪ <i>Do not</i> designate any slots for scan operations in the iKVM GUI Setup Scan menu. iKVM may not work correctly otherwise. ▪ <i>Do not</i> designate any slots for broadcast keyboard/mouse operations in the iKVM GUI Setup Broadcast menu. iKVM may not work correctly otherwise. ▪ Designate a single key sequence to invoke the iKVM GUI. This key sequence must also be identified during KX III port configuration. Otherwise, indiscriminate iKVM operation may occur as a result of client key entry. ▪ Ensure that Front Panel USB/Video Enabled is <i>not</i> selected during iKVM configuration via the Dell CMC GUI. Otherwise, connections made at the front of chassis will take precedence over the KX III connection at the rear, preventing proper iKVM operation. A message will be displayed stating 'User has been disabled as front panel is currently active.' ▪ Ensure that 'Allow access to CMC CLI from iKVM' is <i>not</i> selected during iKVM configuration via the Dell CMC GUI. ▪ To avoid having the iKVM GUI display upon connecting to the blade chassis, set the Screen Delay Time to 8 seconds. ▪ Recommend that 'Timed' and 'Displayed' be selected during iKVM GUI Flag Setup. This will allow you to visually confirm the connection to the desired blade slot.
Dell PowerEdge 1855/1955	▪ Disable the iKVM GUI screensaver. An Authorize dialog will appear if this is not done and will prevent the iKVM from operating correctly. ▪ Exit the iKVM GUI menu before attaching Dell's chassis to a Raritan CIM. iKVM may not work correctly if this is not done. ▪ Configure the iKVM GUI Main menu to select target blades by Slot, not by Name. iKVM may not work correctly if this is not done. ▪ <i>Do not</i> designate any slots for scan operations in the iKVM GUI Setup Scan menu or the iKVM may not work properly. ▪ To avoid having the iKVM GUI display upon connecting to the

Blade chassis	Required/recommended action
	blade chassis, set the Screen Delay Time to 8 seconds. Recommend that 'Timed' and 'Displayed' be selected during iKVM GUI Flag Setup. This will allow you to visually confirm the connection to the desired blade slot.
IBM®/Dell® Auto-Discovery	- It is recommended that Auto-Discovery be enabled when applying blade level access permissions. Otherwise, set access permissions on a blade-chassis wide basis. - Secure Shell (SSH) must be enabled on the blade chassis management module. - The SSH port configured on the blade chassis management module and the port number entered on the Port Configuration page must match.
IBM KX3 Virtual Media	Raritan KX III virtual media is supported only on IBM BladeCenter® Models H and E. This requires the use of the D2CIM-DVUSB. The black D2CIM-DVUSB Low-Speed USB connector is attached to the Administrative Management Module (AMM) at the rear of the appliance. The gray D2CIM-DVUSB High-Speed USB connector is attached to the Media Tray (MT) at the front of the appliance. This will require a USB extension cable.
Cisco® UCS Server Chassis	- The Cisco KVM cable (N20-BKVM) enables you to perform server blade administration, configuration, and diagnostic procedures by connecting video and USB devices directly to the server blade. - Source: <i>Cisco UCS 5108 Server Chassis Installation Guide-DCIM-USBG2, D2CIM-VUSB, D2CIM-DVUSB</i>

Note: All IBM BladeCenters that use AMM must use AMM firmware version BPET36K or later to work with the KX III.

Note: In the case of IBM Blade Center Models E and H, the KX III only supports auto-discovery for AMM[1] as the acting primary management module.

Blade Chassis Sample URL Formats

This table contains sample URL formats for blade chassis being configured in the KX III.

Blade chassis	Sample URL format
Dell® M1000e	- URL: https://192.168.60.44/cgi-bin/webcgi/login - Username: root - Username Field: user

Blade chassis	Sample URL format
	• Password: calvin • Password Field: password
Dell 1855	• URL: https://192.168.60.33/Forms/f_login • Username: root • Username Field: TEXT_USER_NAME • Password: calvin • Password Field: TEXT_PASSWORD
IBM® BladeCenter® E or H	• http://192.168.84.217/private/welcome.ssi

Configuring USB Profiles (Port Page)

You choose the available USB profiles for a port in the Select USB Profiles for Port section of the Port page. The USB profiles chosen in the Port page become the profiles available to the user in VKC when connecting to a KVM target server from the port. The default is the Windows 2000® operating system, Windows XP® operating system, Windows Vista® operating system profile. For information about USB profiles, see **USB Profiles** (on page 54, on page 265).

*Note: To set USB profiles for a port, you must have a digital CIM, VM-CIM or Dual VM-CIM connected with firmware compatible with the current firmware version of the KX III. See **Upgrading CIMs** (on page 212).*

The profiles available to assign to a port appear in the Available list on the left. The profiles selected for use with a port appear in the Selected list on the right. When you select a profile in either list, a description of the profile and its use appears in the Profile Description field.

In addition to selecting a set of profiles to make available for a KVM port, you can also specify the preferred profile for the port and apply the settings from one port to other KVM ports.

*Note: See **Mouse Modes when Using the Mac Boot Menu** (on page 60) for information on using the Mac OS-X® USB profile if you are using a DCIM-VUSB or DCIM-DVUSB virtual media CIM.*

► To open the Port page:

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.

2. Click the Port Name for the KVM port you want to edit. The Port page opens.

► **To select the USB profiles for a KVM port:**

1. In the Select USB Profiles for Port section, select one or more USB profiles from the Available list.
 - Shift-Click and drag to select several continuous profiles.
 - Ctrl-Click to select several discontinuous profiles.
2. Click Add. The selected profiles appear in the Selected list. These are the profiles that can be used for the KVM target server connected to the port.

► **To specify a preferred USB profile:**

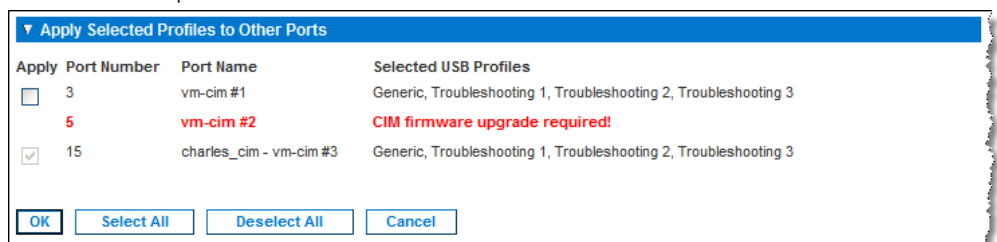
1. After selecting the available profiles for a port, choose one from the Preferred Profile for Port menu. The default is Generic. The selected profile is used when connecting to the KVM target server. You can change to any other USB profile as necessary.
2. If check box Set Active Profile As Preferred Profile is selected, this preferred USB is also used as active profile.

► **To remove selected USB profiles:**

1. In the Select USB Profiles for Port section, select one or more profiles from the Selected list.
 - Shift-Click and drag to select several continuous profiles.
 - Ctrl-Click to select several discontinuous profiles.
2. Click Remove. The selected profiles appear in the Available list. These profiles are no longer available for a KVM target server connected to this port.

► **To apply a profile selection to multiple ports:**

1. In the Apply Selected Profiles to Other Ports section, select the Apply checkbox for each KVM port you want to apply the current set of selected USB profiles to.



- To select all KVM ports, click Select All.
- To deselect all KVM ports, click Deselect All.

Configuring KX III Local Port Settings

Note: Some changes you make to the settings on the Local Port Settings page restart the browser you are working in. If a browser restart occurs when a setting is changed, it is noted in the steps provided here.

► To configure the local port settings:

- Choose Device Settings > Local Port Settings. The Local Port Settings page opens.

Enable Standard Local Port

1. Select the checkbox next to the Enable Standard Local Port to enable it. Deselect the checkbox to disable it.

By default, the standard local port is enabled but can be disabled as needed.

The browser is restarted when this change is made.

Note: If you are using the tiering feature, the Standard Local Port feature will be turned off since both features cannot be used at the same time.



Enable Local Port Device Tiering

1. If you are using the tiering feature, select the Enable Local Port Device Tiering checkbox and enter the tiered secret word in the Tier Secret field.

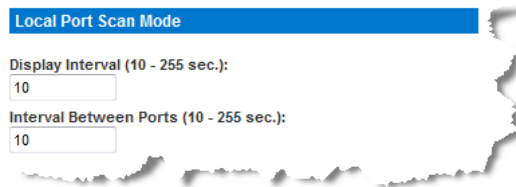
In order to configure tiering, you must also configure the base device on the Device Services page.

See **Configuring and Enabling Tiering** (on page 145) for more information on tiering.



Configure the Local Port Scan Mode Settings

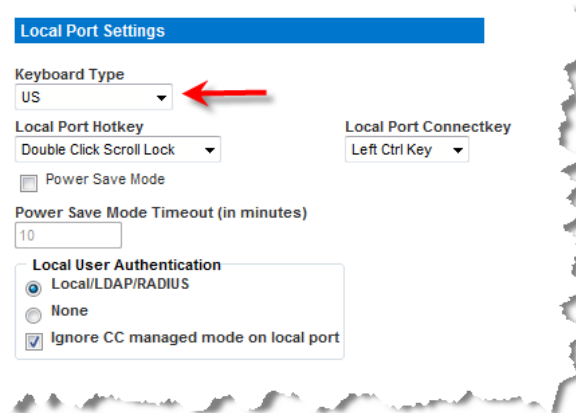
1. If needed, configure the Local Port Scan Mode settings. These settings apply to Scan Settings feature, which is accessed from the Port page.
 - In the "Display Interval (10-255 sec):" field, specify the number of seconds you want the target that is in focus to display in the center of the Port Scan window.
 - In the "Interval Between Ports (10 - 255 sec):" field, specify the interval at which the device should pause between ports.



Select the Local Console Keyboard Type

1. Choose the appropriate keyboard type from among the options in the drop-down list.

The browser will be restarted when this change is made.



- US
- US/International
- United Kingdom
- French (France)
- German (Germany)
- German (Switzerland)
- Simplified Chinese
- Traditional Chinese
- Dubeolsik Hangul (Korean)
- JIS (Japanese Industry Standard)
- Portuguese (Portugal)
- Norwegian (Norway)
- Swedish (Sweden)
- Danish (Denmark)
- Belgian (Belgium)
- Hungarian
- Spanish
- Italian
- Slovenian

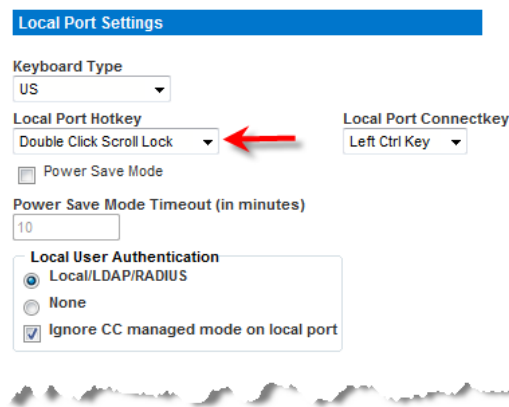
Note: Keyboard use for Chinese, Japanese, and Korean is for display only. Local language input is not supported at this time for KX III Local Console functions.

Note: If using a Turkish keyboard, you must connect to a target server through the Active KVM Client (AKC). It is not supported by other Raritan clients.

Select the Local Port Hotkey

1. Choose the local port hotkey. The local port hotkey is used to return to the KX III Local Console interface when a target server interface is being viewed. The default is to Double Click Scroll Lock, but you can select any key combination from the drop-down list:

Hot key:	Take this action:
Double Click Scroll Lock	Press Scroll Lock key twice quickly
Double Click Num Lock	Press Num Lock key twice quickly
Double Click Caps Lock	Press Caps Lock key twice quickly
Double Click Left Alt key	Press the left Alt key twice quickly
Double Click Left Shift key	Press the left Shift key twice quickly
Double Click Left Ctrl key	Press the left Ctrl key twice quickly



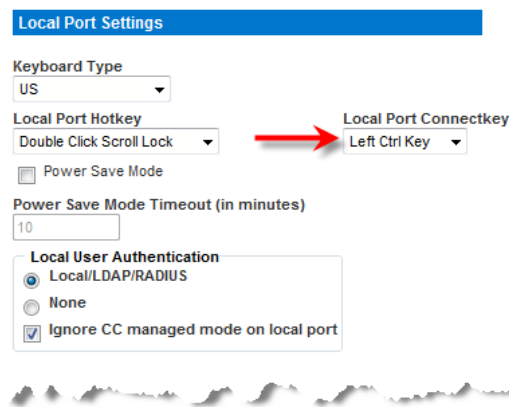
Select the Local Port Connect Key

Select the Local Port Connect key. Use a connect key sequence to connect to a target and switch to another target without returning to the GUI.

Then use the hot key to disconnect and return to the local port GUI

Once the local port connect key is created, it will appear in the Navigation panel of the GUI so you can use it as a reference. See ***Connect Key Examples*** (on page 387) for examples of connect key sequences.

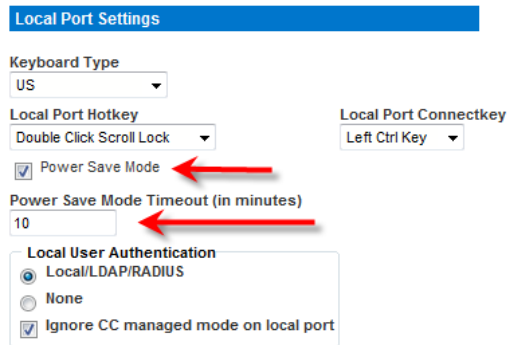
The connect key works for both standard servers and blade chassis.



Configure the Power Save Feature (Optional)

1. If you would like to use the power save feature:
 - a. Select the Power Save Mode checkbox.

- b. Set the amount of time (in minutes) in which Power Save Mode will be initiated.



Local Port Settings

Keyboard Type
US

Local Port Hotkey
Double Click Scroll Lock

Local Port Connectkey
Left Ctrl Key

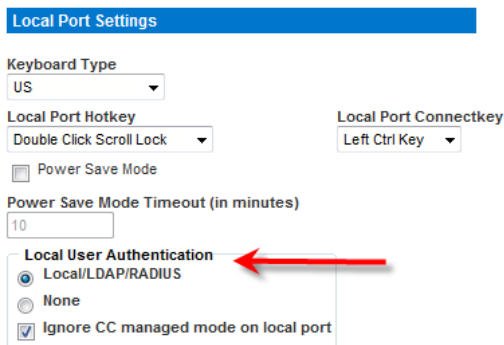
☒ Power Save Mode

Power Save Mode Timeout (in minutes)
10

Local User Authentication
☒ Local/LDAP/RADIUS
☐ None
☒ Ignore CC managed mode on local port

Select the Local User Authentication

1. Choose the type of local user authentication.
 - Local/LDAP/RADIUS. This is the recommended option.
 - None. There is no authentication for Local Console access. This option is recommended for secure environments only.



Local Port Settings

Keyboard Type
US

Local Port Hotkey
Double Click Scroll Lock

Local Port Connectkey
Left Ctrl Key

☐ Power Save Mode

Power Save Mode Timeout (in minutes)
10

Local User Authentication
☒ Local/LDAP/RADIUS
☐ None
☒ Ignore CC managed mode on local port

Device Services

Enabling SSH

Enable SSH access to allow administrators to access the KX III via the SSH v2 application.

► To enable SSH access:

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Select Enable SSH Access.

3. Enter the SSH Port information. The standard SSH TCP port number is 22 but the port number can be changed to provide a higher level of security operations.
4. Click OK.

HTTP and HTTPS Port Settings

You are able to configure HTTP and/or HTTPS ports used by the KX III. For example, if you are using the default HTTP port 80 for another purpose, changing the port will ensure the device does not attempt to use it.

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Enter the new ports in the HTTP Port and/or HTTPS Port fields.
3. Click OK.

Entering the Discovery Port

KX III discovery occurs over a single, configurable TCP Port.

The default is Port 5000, but you can configure it to use any TCP port except 80 and 443.

To access KX III from beyond a firewall, your firewall settings must enable two-way communication through the default Port 5000 or a non-default port configured on this page.

via Remote Console or command line interface (CLI).

► To enable the discovery port:

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Enter the Discovery Port.
3. Click OK.

Configuring and Enabling Tiering

The tiering feature allows you to access KX III targets and PDUs through one base KX III device.

Devices can be added and removed from a tiering configuration as needed up to a maximum of two tiered levels.

When setting up the devices, you will use specific CIMS for specific configurations.

Port configuration, including changing the CIM name, must be done directly from each device. It cannot be done from the base device for tiered target ports.

Tiering also supports the use of KVM switches to switch between servers. See **Configuring KVM Switches** (on page 100).

Once configured, base and tiered devices are displayed on the Port Access Page. See Tiered Devices - Port Access Page

Before Creating a Tiering Configuration

Before creating a tiering configuration, review **Permitted KX III Tiering Configurations** (on page 145) and Unsupported and Limited Features on Tiered Targets.

Before adding tiered devices to a KX III tiering configuration:

- Base and tiered devices must all be operating with the same firmware revision.
- Enable base devices on the Device Settings page. See **Configuring Standard Target Servers** (on page 99)
- Enable tiered devices on the Local Port Settings page. See **Configuring KX III Local Port Settings** (on page 139), then **Enable Local Port Device Tiering** (on page 139)
- Enable tiering for the base device, and the tiered devices. See **Enabling Tiering** (on page 147)

Permitted KX III Tiering Configurations

Before tiering devices, review **Before Creating a Tiering Configuration** (on page 145).

Following are the permitted tiering configurations for KX III:

- KX III base device > KX III tiered devices
- KX III base device > KX II tiered devices
- Dual Video port targets attached to a tier device should be connected via tier devices

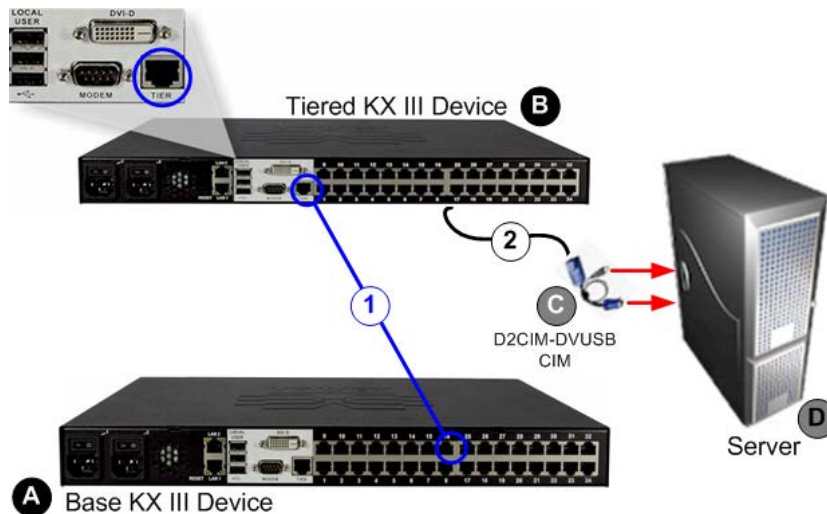
Unsupported and Limited Features on Tiered Targets

The following features are not supported on tiered targets:

- Blade chassis on tiered devices
- Audio on tiered devices
- Smart cards on tiered devices
- Virtual media tiered devices
- DSAM on tiered devices
- MCCAT as a tiered device
- Port group management is limited to creating port groups of members directly attached to the base
- Dual Video port targets attached to a tier device should not be connected through the tier base device
- Absolute Mouse Synchronization may not synch correctly if your tiering configuration consists of a mix of KX III and KX II devices
- A KX II base device > KX III tiered devices

Tiered KX III Connection Example

The following diagram illustrates the cabling configurations between a KX III tiered device and a KX III base device.



Steps	
A	KX III Base device
B	KX III Tiered device
C	CIM to connect the target server to KX III the Tiered device.
D	Target server
1	Base device Tier port to Tiered device Tier port connection: - Connect one end of a Cat5/5e/6 cable into a target server port on the KX III Base device. - Connect the other end of the cable into the Tier port on the KX III Tiered device.
2	Tiered device connection to the target server keyboard/video/mouse ports: - Connect one end of a Cat5/5e/6 cable into a target server port on the KX III Tiered device, and the other end into a supported CIM such as the D2CIM-DVUSB. - Connect the keyboard, mouse and video plugs on the CIM to the corresponding ports on the target server.

Enabling Tiering

1	From the base KX III tier device, select Device Settings > Device Services to open the Device Service Settings page.
2	Select Enable Tiering as Base.
3	In the Base Secret field, enter the secret shared between the base and the tiered devices. This secret is required for the tiered devices to authenticate the base device. Enter the same secret word for the tiered device. Click OK.
4	Enable the tiered devices. From the tiered device, choose Device Settings > Local Port Settings.

5	In the Enable Local Ports section of the page, select Enable Local Port Device Tiering.
6	In the Tier Secret field, enter the same secret word you entered for the base device on the Device Settings page. Click OK.

1.

Once devices are enabled and configured, they appear on the Port Access page.

When the KX III is configured to function as a base device or tiered device, they will be displayed as:

- 'Configured As Base Device' in the Device Information section of the left panel of the KX III interface for base devices.
- 'Configured As Tier Device' in the Device Information section of the left panel of the KX III interface for tiered devices.
- The base device will be identified as 'Base' in the left panel of the tiered device's interface under Connect User.
- Target connections to a tier port from the base will be displayed as 2 ports connected.

Remote and Local Access from Tiered Devices

The base device provides remote and local access over a consolidated port list from the Port Access page.

Tiered devices provide remote access from their own port lists.

Local access is not available on the tiered devices when Tiering is enabled.

Accessing a Blade Chassis from a Base Device

Blade chassis attached directly to a KX III base device are accessible.

Power Control from Tiered Devices

You can power on and off targets that are a part of the tiered configuration.

These targets are accessed from the Port Access page.

If targets and outlets are associated, power control is available from the Port Access page.

Targets and PDU outlet associations are limited to those attached to the same KX III.

PDUs attached to the base or tiered KX IIIs are displayed on the Power page drop-down along with the statistics for the selected powerstrip.

Outlet level control is available as well.

Specifically, you can power off outlets that are currently on but you cannot power cycle outlets that are currently off.

Enabling Direct Port Access via URL

Direct Port Access allows users to bypass having to use the KX III's Login dialog and Port Access page.

This feature also provides the ability to enter a username and password directly to proceed to the target, if the username and password is not contained in the URL.

Direct Port Access URL Syntax for the Virtual KVM Client (VKC)

If you are using the Virtual KVM Client (VKC) and direct port access, use one of the following syntaxes for standard ports:

- `https://IPAddress/dpa.asp?username=username&password=password&port=port number&client=vkc`
Or
- `https://IPAddress/dpa.asp?username=username&password=password&portname=port name&client=vkc`

For blade chassis, the port must be designated by both the port number or name, and slot number.

- `https://IPAddress/dpa.asp?username=username&password=password&port=port number-slot number`
For example, port number-slot number is 1-2 where the blade chassis is connected to port 1, slot 2
- `https://IPAddress/dpa.asp?username=username&password=password&port=port name-slot number`

For example, port name-slot number is Port1-2 where the blade chassis is connected to port 1, slot 2

Username and password are optional.

If username and password are not provided, a login dialog will be displayed and, after being authenticated, the user will be directly connected to the target.

The port may be a port number or port name.

If you are using a port name, the name must be unique or an error is reported.

If the port is omitted altogether, an error is reported.

If you are accessing a target that is part of a dual port video group, direct port access uses the primary port to launch both the primary and secondary ports.

Direct port connections to the secondary port are denied, and usual permission rules apply.

For information on the dual port video group feature, see **Creating a Dual Video Port Group** (on page 185) .

Direct Port Access URL Syntax for the Active KVM Client (AKC)

Follow the syntax described to create direct port access URLs for AKC. If you are using Chrome on Windows, you must also enable the "Enable AKC Download Server Certificate Validation" option in Device Settings > Device Services.

If you are using the Active KVM Client (AKC) and direct port access, use:

- `https://IPAddress/dpa.asp?username=username&password=password&port=port number&client=akc`
Or
- `https://IPAddress/dpa.asp?username=username&password=password&port=port name&client=akc`

For blade chassis, the port must be designated by both the port number or name, and slot number.

- `https://IPAddress/dpa.asp?username=username&password=password&port=port number-slot number&client=akc`
For example, port number-slot number is 1-2 where the blade chassis is connected to port 1, slot 2
- `https://IPAddress/dpa.asp?username=username&password=password&port=port name-slot number&client=akc`

For example, port name-slot number is Port1-2 where the blade chassis is connected to port 1, slot 2

Username and password are optional.

If username and password are not provided, a login dialog will be displayed and, after being authenticated, the user will be directly connected to the target.

The port may be a port number or port name.

If you are using a port name, the name must be unique or an error is reported.

If the port is omitted altogether, an error is reported.

If you are accessing a target that is part of a dual port video group, direct port access uses the primary port to launch both the primary and secondary ports.

Direct port connections to the secondary port are denied, and usual permission rules apply.

For information on the dual port video group feature, see **Creating a Dual Video Port Group** (on page 185) .

Enable Direct Port Access

► To enable direct port access:

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Select Enable Direct Port Access via URL if you would like users to have direct access to a target via the Dominion device by passing in the necessary parameters in the URL.
3. Click OK.

Enabling the AKC Download Server Certificate Validation

If you are using the AKC client, you can choose to use the Enable AKC Download Server Certificate Validation feature or opt not to use this feature.

Note: When operating in IPv4 and IPv6 dual stack mode with 'Enable AKC Download Server Certificate Validation' feature, Microsoft® ClickOnce® requires that the server certificate CN should not contain a zero compressed form of IPv6 address.

If it does, you will not be able to successfully download and launch AKC.

However, this may conflict with browser preferences for the form of the IPv6 address.

Use the server hostname in the common name (CN) or include compressed and uncompressed forms of the IPv6 address in the certificate's Subject Alternative Name.

Option 1: Do Not Enable AKC Download Server Certificate Validation (default setting)

If you do not enable, AKC Download Server Certificate Validation, all Dominion device users and CC-SG Bookmark and Access Client users must:

- Ensure the cookies from the IP address of the device that is being accessed are not currently being blocked.
- Windows Vista, Windows 7 and Windows 2008 server users should ensure that the IP address of the device being accessed is included in their browser's Trusted Sites Zone and that Protected Mode is not on when accessing the device.

Option 2: Enable AKC Download Server Certificate Validation

If you do, enable AKC Download Server Certificate Validation:

- Administrators must upload a valid certificate to the device or generate a self-signed certificate on the device. The certificate must have a valid host designation.
- Each user must add the CA certificate (or a copy of self-signed certificate) to the Trusted Root CA store in their browser.
- When using CC-SG neighborhoods, you must enable AKC on each neighborhood member.

► To install the self-signed certificate when using Windows Vista® operating system and Windows 7® operating system:

1. Include the KX III IP address in the Trusted Site zone and ensure 'Protected Mode' is off.

2. Launch Internet Explorer® using the KX III IP address as the URL. A Certificate Error message will be displayed.
3. Select View Certificates.
4. On the General tab, click Install Certificate. The certificate is then installed in the Trusted Root Certification Authorities store.
5. After the certificate is installed, the KX III IP address should be removed from the Trusted Site zone.

► **To enable AKC download server certificate validation:**

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Select the Enable AKC Download Server Certificate Validation checkbox or you can leave the feature disabled (default).
3. Click OK.

If you are connecting to a KX III standalone device and support for AKC download server certificate validation is enabled, the valid IPv6 format to generate the certificate is either:

- CN =[fd07:02fa:6cff:2500:020d:5dff:fe00:01c0] when there is a leading 0
- or
- CN =[fd07:02fa:6cff:2500:020d:5dff:0000:01c0] when there is no zero compression

Enable Standalone VKC Download Server Certificate Validation

On the Services page select the "Enable Standalone VKC Download Server Certificate Validation" checkbox to use HTTPS for download the VKCs application. JRE will perform a check to ensure the server certificate matches the designated device. If the certification does not match, a security warning message displays to give you the option to continue. Best practice for using VKCs is to select this option, and install a valid certificate on KX III.

When this option is not selected, the VKCs certificate is not validated.

Configuring SNMP Agents

SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP managers. See *Viewing the KX III MIB* (on page 174) for information on viewing the KX III MIB.

KX III supports SNMP logging for SNMP v1/v2c and/or v3. SNMP v1/v2c defines message formats and protocol operations when SNMP logging is enabled. SNMP v3 is a security extension of SNMP that provides user authentication, password management and encryption.

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Provide the following SNMP agent identifier information for the MIB-II System Group objects:
 - System Name - the SNMP agent's name/appliance name
 - System Contact - the contact name related to the appliance
 - a. System Location - the location of the appliance
3. Select either or both Enable SNMP v1/v2c and Enable SNMP v3. At least one option must be selected. **Required**
4. Complete the following fields for SNMP v1/v2c (if needed):
 - Community - the appliance's community string
 - a. Community Type - grant either Read-Only or Read-Write access to the community users

Note: An SNMP community is the group to which appliances and management stations running SNMP belong. It helps define where information is sent. The community name is used to identify the group. The SNMP device or agent may belong to more than one SNMP community.

5. Complete the following fields for SNMP v3 (if needed):
 - Select Use Auth Passphrase if one is needed. If the Privacy Passphrase is required, the 'Use Auth Passphrase' allows you to have the same passphrase for both without having to re-enter the Auth Passphrase.
 - Security Name - the username or service account name of the entity communicating with the SNMP agent (up to 32 characters).
 - Authentication Protocol - the MD5 or SHA authentication protocol used by the SNMP v3 agent.
 - Authentication Passphrase - the pass phrase required to access the SNMP v3 agent (up to 64 characters).
 - Privacy Protocol - if applicable, the AES or DES algorithm used to encrypt PDU and context data.

- a. Privacy Passphrase - if applicable, the pass phrase used to access the privacy protocol algorithm (up to 64 characters).
6. Click OK to start the SNMP agent service.

Configure SNMP traps on the Event Management - Settings page, which can be quickly accessed by clicking the SNMP Trap Configuration link. See **Configuring SNMP Traps** (on page 167) for information on creating SNMP traps and **List of KX III SNMP Traps** (on page 169) for a list of available KX III SNMP traps.

The events that are captured once an SNMP trap is configured are selected on the Event Management - Destination page. See **Configuring Event Management - Destinations** (on page 175).

SNMP Agent Configuration

☐ Enable SNMP Daemon

System Name: DominionKX System Contact: System Location:

☒ Enable SNMP v1/v2c;

Community: Community Type: Read-Only

☐ Enable SNMP v3 ☐ Use Auth Passphrase

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

[Link to SNMP Trap Configuration](#)

► **To reset to factory defaults:**

- Click Reset To Defaults. All items on the page are set back to their defaults.

WARNING: When using SNMP traps over UDP, it is possible for the KX III and the router that it is attached to fall out of synchronization when the KX III is rebooted, preventing the reboot completed SNMP trap from being logged.

Configuring Modem Settings

See ***Certified Modems*** (on page 434) for information on certified modems that work with the KX III.

For information on settings that will give you the best performance when connecting to the KX III via modem, see ***Configuring Connection Properties*** (on page 260).

► To configure modem settings:

1. Click Device Settings > Modem Settings to open the Modem Settings page.
2. Select the Enable Modem checkbox. This will enable the Serial Line Speed and Modem Init String field.
3. The Serial Line Speed of the modem is set to 115200.
4. Enter the initial modem string in the Modem Init String field. If the modem string is left blank, the following string is sent to the modem by default: ATZ OK AT OK.

This information is used to configure modem settings. Because different modems have different ways of settings these values, this document does not specify how to set these values, rather the user should refer to the modem to create the appropriate modem-specific string.

- a. Modem Settings:
 - Enable RTS/CTS flow control
 - Send data to the computer on receipt of RTS
 - CTS should be configured to only drop if required by flow control.
 - DTR should be configured for Modem resets with DTR toggle.
 - DSR should be configured as always on.
 - DCD should be configured as enabled after a carrier signal is detected. (that is, DCD should only be enabled when modem connection is established with the remote side)
5. Enter the IPv4 modem server address in the Modem Server IPv4 Address field and the client modem address in the Modem Client IPv4 Address field.

Note: The modem client and server IP addresses must be on the same subnet and cannot overlap the device's LAN subnet.

- Click OK to commit your changes or click Reset to Defaults to return the settings to their defaults.

Home > Device Settings > Modem Settings

Modem Settings

☒ **Enable Modem**

Serial Line Speed

115200

 bits/s

Modem Init String

ATQMB122L

Modem Server IPv4 Address

10.0.0.1

Modem Client IPv4 Address

10.0.0.2

OK

Reset To Defaults

Cancel

Connect and Enable Global Access to an External USB-Connected Broadband Modem

Users who need access to KX III via the Sierra Wireless modem must be assigned to a user group with Modem Access permissions. This is a security measure that helps control who can access KX III via the modem. For example, create a user group called Sierra Wireless Users and give the group Modem Access permissions, then assign only users who need access to the modem to that group.

The Enable Broadband Modem feature must be enabled in KX III in order for users to access KX III via the Sierra Wireless modem. This is a global-level feature, so it is disabled by default in order to prevent all users from being able to access KX III via the modem.

Sierra Wireless Software and Firmware Versions

Sierra Wireless must have at least ALEOS Software Version 4.4.1.014

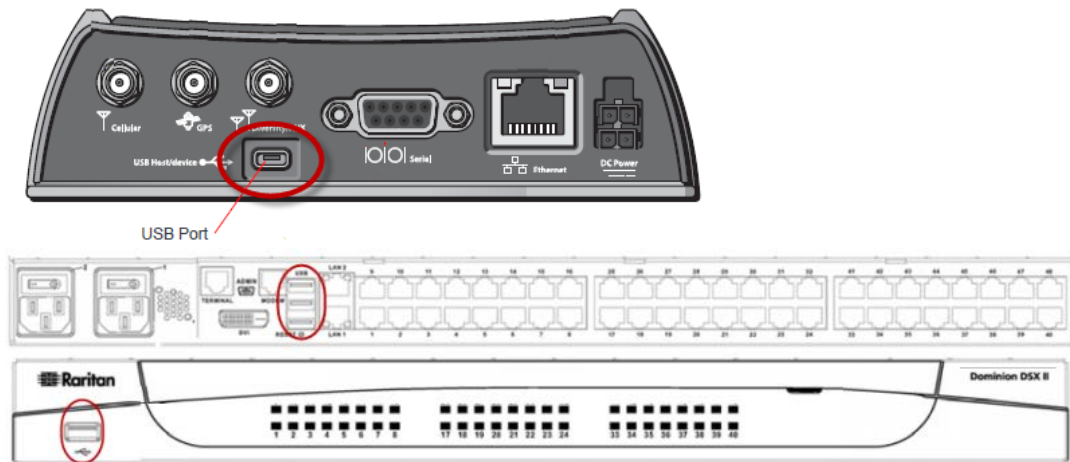
Raritan has tested this configuration with the Verizon Wireless MC7750 Radio Module using firmware version 3.05.10.13.

Connect the External, Wireless Modem

USB Connection

Use either a Micro A or Micro B to USB Type A cable to connect the Sierra Wireless to the KX III.

- Connect the Sierra Wireless USB port to any of the three USB ports on back of the KX III or to the USB port on the front of the KX III.



Note: Only USB connections are supported for this modem.

Configure the Sierra Wireless Modem

Configure the Sierra Wireless modem for use with KX III using these connections. These settings are configured on the Sierra Wireless modem, not KX III.

Configure the Sierra Wireless Modem for a Cellular Connection

- A SIM card must be purchased from your service provider and installed in the Sierra Wireless modem.
- Get a static IP address from our service provider, then assign it to the Sierra Wireless modem.
- Sierra Wireless must be configured for Public mode.
- Host Connection Mode must be set to "USB Uses Public IP".
- USB Device Mode must be set to "USBNET".

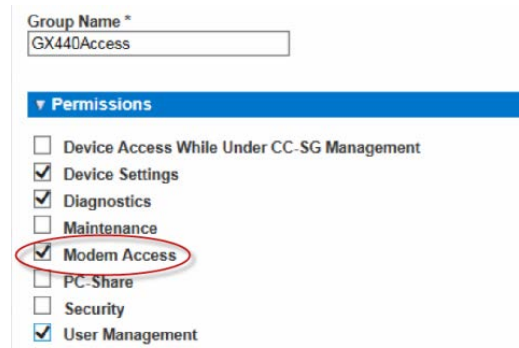
Change Default Username

For security reasons, Raritan recommends you change the default Admin account username to a new name before using the Sierra Wireless .

Assign User Groups Modem Access Permissions

Following are settings applied in KX III.

- Modem Access permission is assigned to a user group on the Group page, and the user is then assigned to the group on the User page. For more information, see User Profiles and Groups.



Group Name *

GX440Access

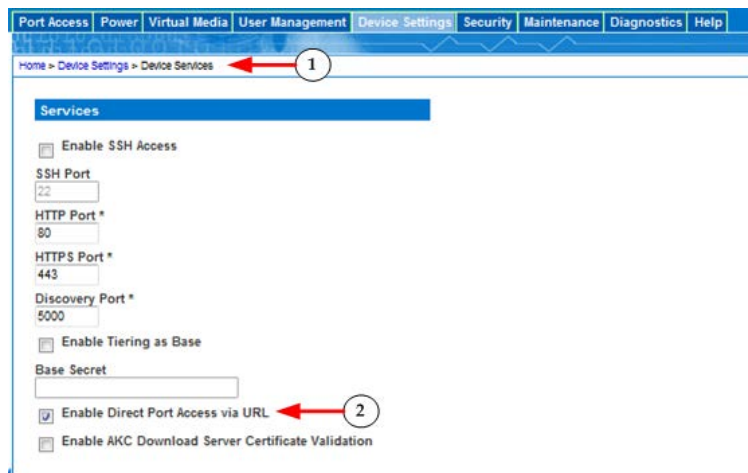
▼ Permissions

- ☐ Device Access While Under CC-SG Management
- ☒ Device Settings
- ☒ Diagnostics
- ☐ Maintenance
- ☒ Modem Access
- ☐ PC-Share
- ☐ Security
- ☒ User Management

Configure Settings to Access KX III via Modem through Direct Port Access

For modem access through direct port access, you must configure settings in:

- The KX III remote console
- On the client machine in the Java Control Panel and in your browser (Microsoft Internet Explorer® and Firefox® information is provided here)
- In the Virtual KVM Client (VKC)



Steps

1	In KX III, select Device Settings > Device Services to open the Device Services page.
2	Select “Enable Direct Port Access via URL”.

Port Access Power Virtual Media User Management Device Settings Security Maintenance Diagnostics Help

Home > Security > Security Settings

Login Limitations

- ☐ Enable Single Login Limitation
- ☐ Enable Password Aging
- Password Aging Interval (days)
80
- ☐ Log Out Idle Users
- Idle Timeout (minutes)
30

Strong Passwords

- ☐ Enable Strong Passwords
- Minimum length of strong password
8
- Maximum length of strong password
16
- ☒ Enforce at least one lower case character
- ☒ Enforce at least one upper case character
- ☒ Enforce at least one numeric character
- ☒ Enforce at least one printable special character
- Number of restricted passwords based on history
5

User Blocking

- ☐ Disabled
- ☐ Timer Lockout
- Attempts
3
- Lockout Time
5
- ☐ Deactivate User-ID
- Failed Attempts
3

Encryption & Share

Encryption Mode
Auto

- ☒ Apply Encryption Mode to KVM and Virtual Media (Forced in FIPS 140-2 Mode)
- ☒ Enable FIPS 140-2 Mode (Changes are activated on reboot only!)

Current FIPS status: Inactive

PC Share Mode
Private

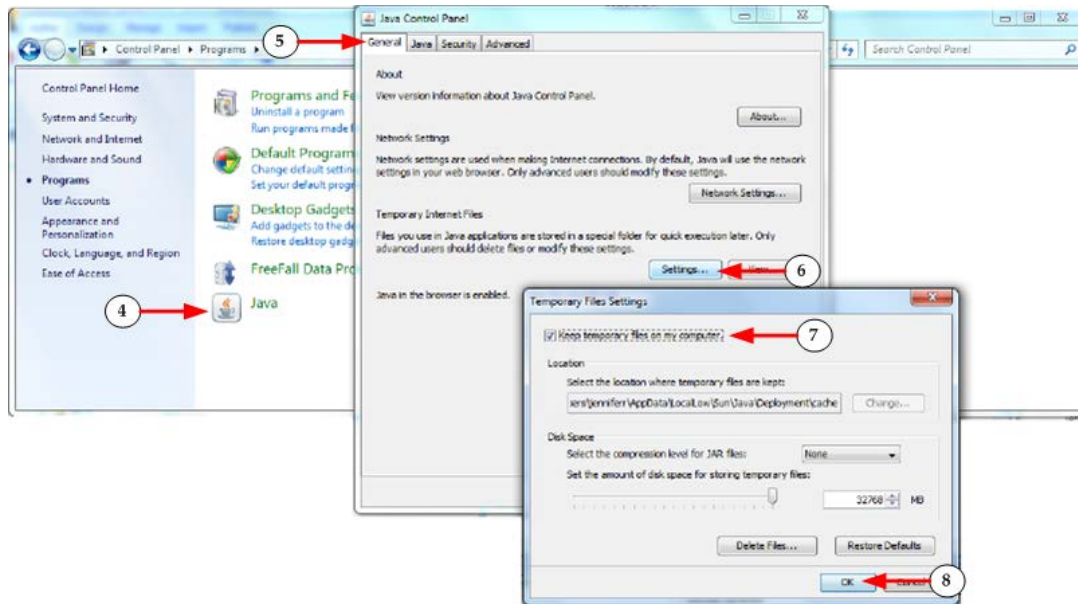
- ☐ VM Share Mode

Local Device Reset Mode
Enable Local Factory Reset

Steps

- 3 For better modem performance, deselect the “Apply Encryption Mode to KVM and Virtual Media (Forced in FIPS 140-2 Mode)” setting if it is enabled on the Security Settings page (select Security > Security Settings). **Optional**

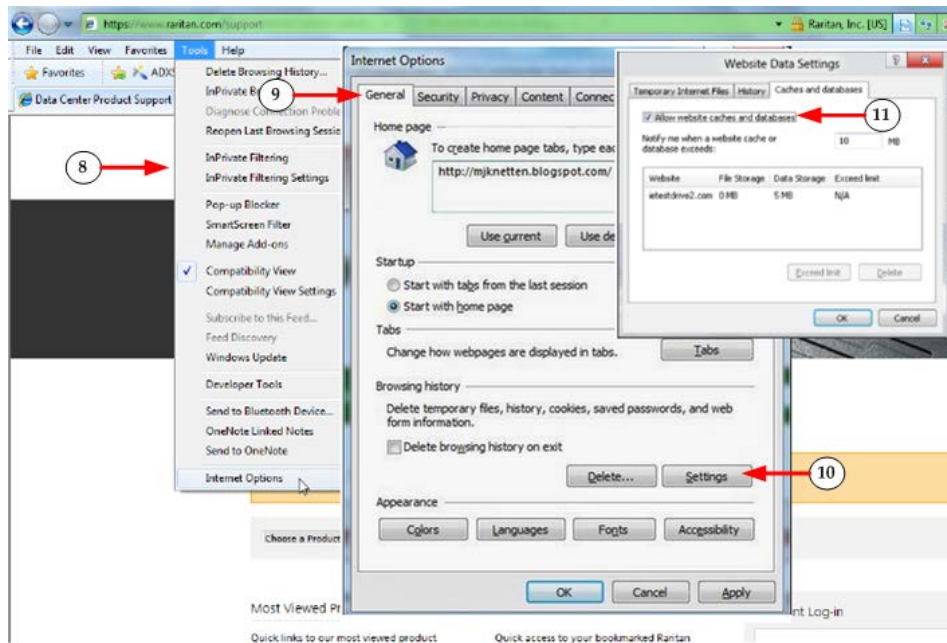
Configure the following Java security settings on your client machine. The steps here use a Windows® machine as an example.



Steps

④	Access the Java Control Panel from the Microsoft Windows® Control Panel.
⑤	In the Java Control Panel, open to the General tab.
⑥	Click Settings.
⑦	Select "Keep temporary files on my computer".
⑧	Click OK. You can now close the Java Control Panel and Microsoft Control Panel.

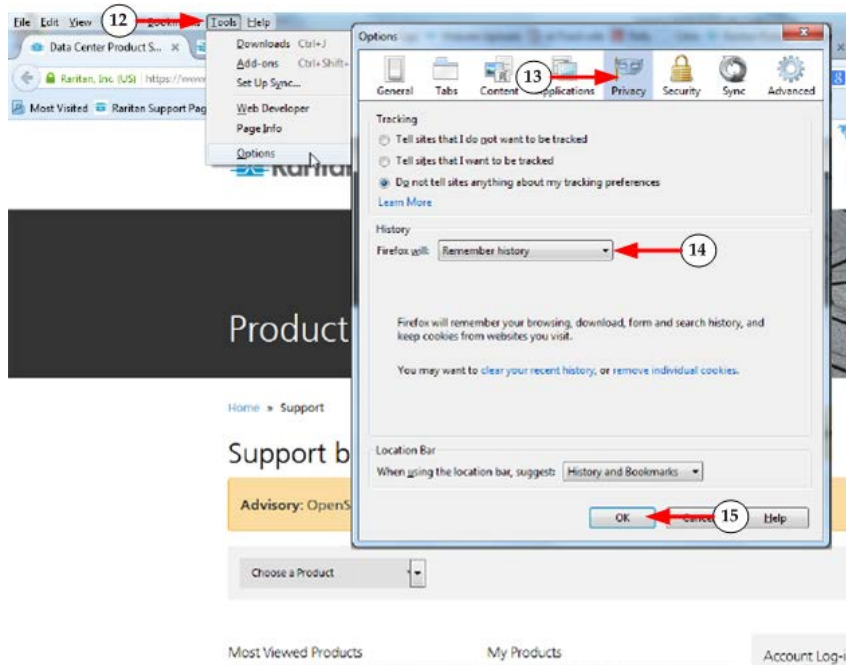
Configure the following browser settings on your client machine, depending on the browser you use.



Steps

8	For Microsoft Internet Explorer®, click Tools > Internet Options. The steps here follow Internet Explorer 9.
9	Click on the General tab.
10	Click Settings in the Browser History section to open the Windows Database Settings dialog.
11	Click the "Caches and Databases" tab and select "Allow website caches and databases" to enable the cache in the browser. Click OK on the Windows Database Settings dialog and the Internet Options dialog to apply the settings

Chapter 3: KX III Interface and Navigation

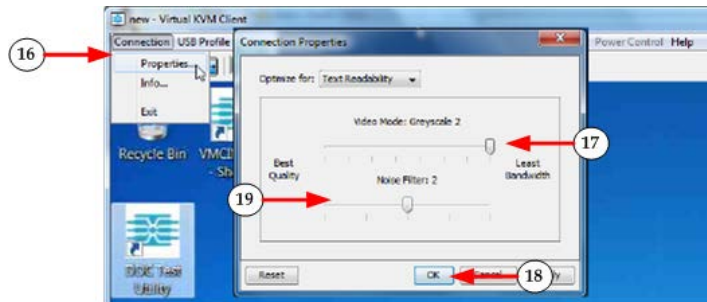


Steps	
12	For Firefox®, click Tools > Options.
13	Click on Privacy.
14	Set the History to "Firefox will" to "Remember history".
15	Click OK to apply the settings.

Finally, you need to perform the following steps the first time you access each target server via the Virtual KVM Client (VKC) from KX III. Settings only need to be applied once.

The first time you attempt to connect to each target via VKC, the connection fails. This is because the session times out when the Java applet is downloaded via direct port access.

Connect to the target a second time, and the VKC is launched successfully.



Steps

16	In VKC, click Connection > Properties to open the Connection Properties dialog.
17	Set the Video Mode to “Greyscale 2” so you use the least bandwidth.
18	Click OK.
19	It may be necessary to set the “Noise Filter” to greater than 2 if the modem connection is slow after you test it.

Configuring Date/Time Settings

Use the Date/Time Settings page to specify the date and time for the KX III. There are two ways to do this:

- Manually set the date and time.
- Synchronize the date and time with a Network Time Protocol (NTP) server.

► To set the date and time:

1. Choose Device Settings > Date/Time. The Date/Time Settings page opens.
2. Choose your time zone from the Time Zone drop-down list.
3. Adjust for daylight savings time by checking the “Adjust for daylight savings time” checkbox.
4. Choose the method to use to set the date and time:

- User Specified Time - use this option to input the date and time manually. For the User Specified Time option, enter the date and time. For the time, use the hh:mm format (using a 24-hour clock).
 - Synchronize with NTP Server - use this option to synchronize the date and time with the Network Time Protocol (NTP) Server.
5. For the Synchronize with NTP Server option:
- a. Enter the IP address of the Primary Time server.
 - b. Enter the IP address of the Secondary Time server. **Optional**

Note: If DHCP is selected for the Network Settings on the Network page, the NTP server IP address is automatically retrieved from the DHCP server by default. Manually enter the NTP server IP address by selecting the Override DHCP checkbox.

6. Click OK.

Event Management

The KX III Event Management feature allows you enable and disable the distribution of system events to SNMP Managers, SMTP, the Syslog and the audit log. These events are categorized, and for each event you can determine whether you want the event sent to one or several destinations.

Configuring Event Management - Settings

Configure SNMP traps and the syslog configuration from the Event Management - Settings page. See ***Configuring SNMP Traps*** (on page 167).

Once configured, enable the SNMP traps on the Event Management - Destinations page. See ***Configuring Event Management - Destinations*** (on page 175).

Configuring SNMP Traps

Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions.

SNMP traps are sent out over a network to gather information.

The traps are configured on the Event Management - Settings page. See **List of KX III SNMP Traps** (on page 169) for a list of KX III SNMP traps.

SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and respond to the SNMP trap.

SNMP agents are configured on the Device Services page. See **Configuring SNMP Agents** (on page 154) for information on configuring SNMP agents and **Viewing the KX III MIB** (on page 174) for information on viewing the KX III MIB.

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.
2. Select the SNMP Logging Enabled checkbox to enable to remaining checkboxes in the section. **Required**
3. Select either or both SNMP v1/v2c Traps Enabled and SNMP Trap v3 Enabled. At least one option must be selected.

Once selected, all related fields are enabled. **Required**

4. Complete the following fields for SNMP v1/v2c (if needed):
 - Destination IP/Hostname - the IP or hostname of the SNMP manager. Up to five (5) SNMP managers can be created

Note: IPv6 addresses cannot exceed 80 characters in length for the host name.

- a. Port Number - the port number used by the SNMP manager
- b. Community - the appliance's community string

Note: An SNMP community is the group to which appliances and management stations running SNMP belong. It helps define where information is sent. The community name is used to identify the group. The SNMP device or agent may belong to more than one SNMP community.

5. If it is not already, select the SNMP Trap v3 Enabled checkbox to enable the following fields. Complete the following fields for SNMP v3 (if needed):
 - Destination IP/Hostname - the IP or hostname of the SNMP manager. Up to five (5) SNMP managers can be created

Note: IPv6 addresses cannot exceed 80 characters in length for the host name.

- a. Port Number - the port number used by the SNMP manager
 - Security Name - the username or service account name of the entity communicating with the SNMP agent (up to 32 characters).
 - Authentication Protocol - the MD5 or SHA authentication protocol used by the SNMP v3 agent.
 - Authentication Passphrase - the pass phrase required to access the SNMP v3 agent (up to 64 characters).
 - Privacy Protocol - if applicable, the AES or DES algorithm used to encrypt PDU and context data.
- a. Privacy Passphrase - if applicable, the pass phrase used to access the privacy protocol algorithm (up to 64 characters).

*Note: If you are accessing the Event Management - Settings page from the local console and are using a screen resolution lower than 1280x1024, the Privacy Passphrase column may not be displayed on the page. If this occurs, hide the KX III's left panel. See **Left Panel** (on page 28)*

6. Click OK to create the SNMP traps.

Use the Link to SNMP Agent Configuration link to quickly navigate to the Devices Services page from the Event Management - Settings page.

The events that are captured once an SNMP trap is configured are selected on the Event Management - Destination page. See **Configuring Event Management - Destinations** (on page 175).

KX III supports SNMP logging for SNMP v1/v2c and/or v3. SNMP v1/v2c defines message formats and protocol operations when SNMP logging is enabled. SNMP v3 is a security extension of SNMP that provides user authentication, password management and encryption.

► **To edit existing SNMP traps:**

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.
2. Make changes as needed and click OK to save the changes.

Note: If you disable SNMP settings at any time, the SNMP information is retained so you do not have to reenter if you re-enable the settings.

► **To delete SNMP traps:**

- Clear all of the SNMP trap fields and save.

Use the reset to factory defaults feature to remove the SNMP configuration and set the KX III to its original factory default.

► **To reset to factory defaults:**

- Click Reset To Defaults.

WARNING: When using SNMP traps over UDP, it is possible for the KX III and the router that it is attached to fall out of synchronization when the KX III is rebooted, preventing the reboot completed SNMP trap from being logged.

List of KX III SNMP Traps

SNMP provides the ability to send traps, or notifications, to advise an administrator when one or more conditions have been met.

The following table lists the KX III SNMP traps:

Trap Name	Description
bladeChassisCommError	A communications error with blade chassis device connected to this port was detected.
cimConnected	The CIM is connected.
cimDisconnected	The CIM is disconnected.

Trap Name	Description
cimUpdateStarted	The CIM update start is underway.
cimUpdateCompleted	The CIM update is complete.
configBackup	The device configuration has been backed up.
configRestore	The device configuration has been restored.
deviceUpdateFailed	Device update has failed.
deviceUpgradeCompleted	The KX III has completed update via an RFP file.
deviceUpgradeStarted	The KX III has begun update via an RFP file.
factoryReset	The device has been reset to factory defaults.
firmwareFileDiscarded	Firmware file was discarded.
firmwareUpdateFailed	Firmware update failed.
firmwareValidationFailed	Firmware validation failed.
groupAdded	A group has been added to the KX III system.
groupDeleted	A group has been deleted from the system.
groupModified	A group has been modified.
ipConflictDetected	An IP Address conflict was detected.
ipConflictResolved	An IP Address conflict was resolved.
networkFailure	An Ethernet interface of the product can no longer communicate over the network.
networkParameterChanged	A change has been made to the network parameters.
passwordSettingsChanged	Strong password settings have changed.
portConnect	A previously authenticated user has begun a KVM session.
portConnectionDenied	A connection to the target port was denied.
portDisconnect	A user engaging in a KVM session closes the session properly.
portStatusChange	The port has become unavailable.
powerNotification	The power outlet status notification: 1=Active, 0=Inactive.
powerOutletNotification	Power strip device outlet status notification.

Trap Name	Description
rebootCompleted	The KX III has completed its reboot.
rebootStarted	The KX III has begun to reboot, either through cycling power to the system or by a warm reboot from the OS.
scanStarted	A target server scan has started.
scanStopped	A target server scan has stopped.
securityBannerAction	Security banner was accepted or rejected.
securityBannerChanged	A change has been made to the security banner.
securityViolation	Security violation.
setDateTime	The date and time for the device has been set.
setFIPSMODE	FIPS mode has been enabled.
startCCManagement	The device has been put under CommandCenter Management.
stopCCManagement	The device has been removed from CommandCenter Management.
userAdded	A user has been added to the system.
userAuthenticationFailure	A user attempted to log in without a correct username and/or password.
userConnectionLost	A user with an active session has experienced an abnormal session termination.
userDeleted	A user account has been deleted.
userForcedLogout	A user was forcibly logged out by Admin
userLogin	A user has successfully logged into the KX III and has been authenticated.
userLogout	A user has successfully logged out of the KX III properly.
userModified	A user account has been modified.
userPasswordChanged	This event is triggered if the password of any user of the device is modified.
userSessionTimeout	A user with an active session has experienced a session termination due to timeout.
userUploadedCertificate	A user uploaded a SSL certificate.

Trap Name	Description
vmImageConnected	User attempted to mount either a device or image on the target using Virtual Media. For every attempt on device/image mapping (mounting) this event is generated.
vmImageDisconnected	User attempted to unmount a device or image on the target using Virtual Media.

Enable Email (SMTP) Notifications from the Remote Console

Enable email notifications for users on the Event Management - Settings page.

Each person for whom SMTP is enabled receives notification when an event is triggered. Up to ten (10) users can be added.

Configure SMTP server settings on the SMTP Settings page. Use the "Link to SMTP server configuration" quick link at the bottom of the Event Management - Settings page. See ***Configure and Test SMTP Server Settings*** (on page 173).

► To enable SMTP Notifications:

1. Select Device Settings > Event Management - Settings to open the Event Management - Settings page.
2. Go to the SMTP Settings panel and select the Enable SMTP Server checkbox.

SysLog Configuration

☐ Enable Syslog Forwarding

IP Address/Host Name

SMTP Configuration

☒ SMTP Logging Enabled

Email Subscribers
☐ itemail@raritan.com
☐ raritanemail@raritan.com

New Email Subscriber Address

[Link to SMTP server configuration](#)

3. Type the email address of the SMTP subscriber in the New Email Subscriber Address field and then click Add.
4. Click OK.

Configure and Test SMTP Server Settings

Enter the information required for a connection to your SMTP server on the SMTP Server Settings page.

Note that if the server requires STARTTLS, KX III automatically uses it.

1. Select Device Settings > SMTP Settings.
2. Provide the server address, port and the email address used to send SMTP notifications.
3. If the server requires a username and password authentication to send emails, provide them in the User Account and Password fields, respectively.
4. Click Apply.

Home > Device Settings > SMTP Settings

SMTP Settings

Server
fd07.2fa6cff.2021:3e4a:92ff:

Port
25

Sender Email Address
support@raritan.com

☒ SMTP server requires password authentication

User Account
Support

Password

Apply Reset To Defaults

Test SMTP Settings

Testing will not save changes. Use the apply button when you are satisfied with your settings.

Receiver Address
support@raritan.com Send

It is important that the SMTP server information be accurate so that the KX III appliance can send messages using that SMTP server.

This test sends an email using the settings displayed on the page in the SMTP Settings pane. KX III saves the settings once you click Apply.

1. Send a test email by entering a destination email address to receive the test message

Note that the receiver email is not saved.

2. Verify the message was received by the intended email target. If there are problems, contact your SMTP administrator to make sure your SMTP server IP address and authorization information are correct.

Home > Device Settings > SMTP Settings

SMTP Settings

Server
fd07:2fa:6cff:2021:3e4a:92ff:

Port
25

Sender Email Address
support@raritan.com

☒ SMTP server requires password authentication

User Account
Support

Password

[Apply](#) [Reset To Defaults](#)

Test SMTP Settings

Testing will not save changes. Use the apply button when you are satisfied with your settings.

Receiver Address
support@raritan.com [Send](#)

Viewing the KX III MIB

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.
2. Click the 'Click here to view the 'SNMP MIB' link. The MIB file opens in a browser window.

SysLog Configuration

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.
2. Select Enable Syslog Forwarding to log the appliance's messages to a remote Syslog server.
3. Type the IP Address/Hostname of your Syslog server in the IP Address field.
4. Click OK.

Note: IPv6 addresses cannot exceed 80 characters in length for the host name.

- Click Reset to Defaults at the bottom of the page to remove the setting.

Configuring Event Management - Destinations

If system events are enabled, SNMP notification events (traps) are generated. The events can be logged to the syslog or audit log.

Events and where the event information is sent is configured on the Event Management - Destinations page.

Note: SNMP, Syslog, and SMTP logging only works when enabled in the Event Management - Settings page.

► **To select events and their destinations:**

1. Choose Device Settings > Event Management - Destinations. The Event Management - Destinations page opens.
System events are categorized by Device Operation, Device Management, Security, User Activity, and User Group Administration.
2. Select the checkboxes for those event line items you want to enable or disable, and where you want to send the information.

Tip: Enable or disable entire categories by checking or clearing the Category checkboxes, respectively.

3. Click OK.

► **To reset to factory defaults:**

- Click Reset To Defaults.

WARNING: When using SNMP traps over UDP, it is possible for the KX III and the router that it is attached to fall out of synchronization when the KX III is rebooted, preventing the reboot completed SNMP trap from being logged.

Power Supply Setup

KX III provides dual power supplies, and can automatically detect and provide notification regarding the status of these power supplies.

When both power supplies are used, KX III automatically detects them and notifies you of their status. Additionally, both the PowerIn1 and PowerIn2 Auto Detect checkboxes are automatically selected on the Power Supply Setup page.

If you are using only one power supply, you can enable automatic detection for only the power supply in use.

Proper configuration of power supplies ensures KX III sends the appropriate notifications should a power supply fail. For example, if power supply number one fails, the power LED at the front of the unit will turn red.

The Power LED on the front of the KX III appliance is red when the checkbox is selected for an unconnected power supply. The LED is blue when the checkbox is not selected for an unconnected power supply.

► **To enable automatic detection for the power supplies in use:**

1. Choose Device Settings > Power Supply Setup. The Power Supply Setup page opens.



2. If you are plugging power input into power supply number one (left-most power supply at the back of the unit), then select the PowerIn1 Auto Detect option.
3. If you are plugging power input into power supply number two (right-most power supply at the back of the unit), then select the PowerIn2 Auto Detect option.
4. Click OK.

► **To turn off the automatic detection:**

- Deselect the checkbox for the appropriate power supply.

► **To reset to factory defaults:**

- Click Reset To Defaults.

Note: The KX III does NOT report power supply status to CommandCenter. Dominion I (generation 1), however, does report power supply status to CommandCenter.

Connect and Disconnect Scripts

The KX III provides the ability to execute key macro scripts when connecting to or disconnecting from a target.

You can create and edit your own scripts on the Connection Script page to perform additional actions when connecting to or disconnecting from targets.

Alternatively, you can import existing connection scripts in XML file format. Scripts that you create in KX III can also be exported in XML file format.

A total of 16 scripts can be accommodated on the KX III.

Home > Device Settings > Connection Scripts

Manage Scripts

Available Connection Scripts

Ctrl-Alt-Del_OnExit (Disconnect)
AKC-PrtScr (Connect)

Add

Modify

Remove

Select All

Deselect All

Import

Export

Apply Selected Scripts to Ports

Apply	No.	Name	Scripts Currently in Use
☒	5	SE-IX2-232-LP-ChangedName	
☒	6	Japanese Target	
☒	8	se-ksx2-188-local-port	On Disconnect: Ctrl-Alt-Del_OnExit
☒	9	W2K3 Server	
☒	18	Win XP 2.4GHz P4 504MB	

Select All

Deselect All

Apply Script

Remove Connect Scripts

Remove Disconnect Scripts

OK

Cancel

Applying and Removing Scripts

► To apply a script to targets:

1. Click Device Settings > Connection Scripts. The Connection Scripts page opens.
2. In the Available Connection Scripts section, select the script to be applied to the target(s). One 'On Connect' and one 'On Disconnect' script may be applied to a target.

Note: Only one script can be added to the targets at a time.

3. In the Apply Selected Scripts to Ports section, select the target(s) you want to apply the script to using Select All or clicking on the checkbox to the left of each target to apply the script to only select targets.
4. Click Apply Scripts. Once the script is added to the target, it appears under the Scripts Currently in Use column in the Apply Selected Scripts to Ports section.

► **To remove a script from targets:**

1. In the Apply Selected Scripts to Ports section, select the target(s) you want to remove the scripts from using Select All or clicking on the checkbox to the left of each target to remove the script from only select targets.
2. Click Remove Connect Scripts to remove connect scripts or click Remove Disconnect Scripts to remove disconnect scripts.

Adding Scripts

*Note: You can also add scripts that were created outside of KX III and import them as XML files. See **Importing and Exporting Scripts** (on page 182).*

► **To create script:**

1. Click Device Settings > Connection Scripts. The Connection Scripts page opens.
2. In the Available Connection Scripts section, click Add. The Add Connection Script page opens.
3. Enter a name for the script up to 32 characters in length. This name is displayed in the Available Connection Scripts section of the Configure Scripts page once the script is created.
4. Select either Connect or Disconnect as the type of script you are creating. Connect scripts are used on a new connection or when switching to a target.
5. Select the keyboard type required for the target you are using.
6. From the Key Sets drop-down, choose the keyboard key set you want to use to create the script. Once selected, the Add box below the Key Sets drop-down is populated with the selected key set options.
7. Select a key from the Add box and click Add to move it to Script box. Remove a key from Script box by selecting it clicking Remove. Reorder keys by selecting them and using the Up and Down icons. The script can consist of one or more keys. Additionally, you can mix and match the keys to be used in the script.

For example, select F1-F16 to display the function key set in the Add box. Select a function key and add it to the Script box. Next, select Letters from the Key Set drop-down and add a letter key to the script.

8. Optionally, add text that will display when the script is executed.
 - a. Click Construct Script from Text to open the Construct Script From Text page.
 - b. Enter the script in the text box. For example, enter "Connected to Target".
 - c. Click OK Construct Script From Text page.
9. Click OK to create the script.

Home > Device Settings > Connection Scripts > Add Connection Script

Add Connection Script

Script Name

Use On ☒ Connect ☐ Disconnect

Keyboard Type

Key Sets [Construct Script From Text](#)

Keys	
A	
B	
C	
D	
E	
F	
G	
H	
I	
J	

[Add](#) [Remove](#) [^](#) [v](#)

[OK](#) [Cancel](#) [Clear](#)

Home > Device Settings > Connection Scripts > Modify Connection Script

Construct Script From Text

[OK](#) [Cancel](#) [Clear](#)

Modifying Scripts

► To modify existing scripts:

1. Click Device Settings > Connection Scripts. The Connection Scripts page opens.
2. In the Available Connection Scripts section, select the script you want to modify and click Modify. The page is then in Edit mode.
3. Make changes as needed. Click OK when finished.

Importing and Exporting Scripts

You are able to import and export connect and disconnect scripts that are in XML file format. Keyboard macros cannot be imported or exported.

Note: The import and export feature is not available from the Local Console.

Imported scripts can be edited in KX III using the Modify feature. However, once an imported script is associated with a port, it cannot be modified. Remove the script from the port to modify it. See ***Applying and Removing Scripts*** (on page 178).

► To import a script:

1. Click Device Settings > Connection Scripts. The Connection Scripts page opens.
2. In the Available Connection Scripts section, click Import. The Import Connection Scripts page opens.
3. Select the import setting.
 - Skip duplicates - Scripts that already exist in KX III are not included in the import.
 - Overwrite duplicates - Scripts that already exists in KX III are overwritten by the new, imported script.
 - Add duplicates with a different name - Duplicate scripts will be renamed during the import and will not overwrite existing scripts. KX III assigns a number to the file name to distinguish it from the original.
4. Use the browse function to locate the XML script files to import.

- Click Import. The Configuration Scripts page opens and the imported scripts are displayed.

Home > Device Settings > Connection Scripts > Import Connection Scripts

► **To export a disconnect script:**

- Click Device Settings > Configuration Scripts. The Configuration Scripts page opens.
- In the Available Connection Scripts section, select the script you want to export and click Export. A dialog prompting you to open or save the XML file appears.
- Save the XML file or open it in an XML editor. If you save the XML file, it is saved to your default Download folder.

Port Group Management

Port group management refers to the following:

- Blade Server Group - the aggregation of ports connected to certain types of blades into a group representing the blade chassis. See *HP and Cisco UCS Blade Chassis Configuration (Port Group Management)* (on page 129) for details.
- Dual Video Port Group - the creation of port groups that provide extended desktop configurations on target servers. See *Creating a Dual Video Port Group* (on page 185).
- Port Group - the creation of 'standard' port groups where settings applying to a primary port are applied to all secondary ports in the group. See *Creating Port Groups* (on page 184).

Creating Port Groups

The KX III supports the aggregation of multiple ports into a single port group. Port groups consist solely of ports configured as standard KVM ports.

A port may only be a member of a single group.

Ports that are available to be included in a port group are displayed in the Select Port for Group > Available list.

Once a port is added to a port group, it is not available to add to another port group. Remove the port from its existing port group to use it in a new one.

A maximum of 8 port groups can be created. The Add button is disabled once this limit is reached.

Connect and disconnect actions performed from the primary port are applied to the secondary ports in the group with the exception of power control.

Port Groups are restored using the Backup and Restore option (see Backup and Restore).

*Note: See **HP and Cisco UCS Blade Chassis Configuration (Port Group Management)** (on page 129) for information on creating port groups for blade chassis, and **Creating Dual Port Video Groups** for information on creating dual video port groups.*

► To create a port group:

1. Select Device Settings > Port Group Management. The Port Group Management page opens. Any existing port groups are displayed.
2. Click Add. The page refreshes and displays all of the port group options available.
3. Select the Port Group radio button.
4. Select the ports to add to the group by clicking on them in the Available text box, and then clicking Add to add it to the Selected text box.
5. Click OK to create the port group. The port group now appears on the Port Group Management page.

Creating a Dual Video Port Group

The dual video port groups feature allows you to group two video ports into one group.

Use this feature when you need to connect to a server with two video cards/ports, and you want to access both ports from the same remote client at the same time.

Note: Dual port video groups are not supported by models with only one KVM channel such as KX3-108 and KX3-116 models.

Note: Once a dual video port group is created, it is available from the local console as well as the remote client. However, extended desktop is not supported at the local console.

Dual video port groups appear on the Port Access page as Dual Port types.

The primary and secondary ports that are a part of the port group appear on the Port Access page as Dual Port(P) and Dual Port(S), respectively. For example, if the CIM type is DCIM, "DCIM Dual Port (P)" is displayed.

Each group must contain a primary port and a secondary port.

The configuration applied to the primary port is applied to all secondary ports in the group. If a port is removed from the group, it is considered an independent port and a new configuration can be applied to it.

When you access a dual port video group from the remote client, you connect to the primary port, which opens a KVM connection window to both the primary and secondary ports of the dual port group.

The sessions can be launched and viewed from the remote client on one or multiple monitors as needed.

The orientation setting configured on the device for the target must match the actual configuration on the target operating system.

It is recommended that the connecting client have the same screen orientation whenever possible.

Important: Review the information in the Dual Video Port Groups section for restrictions, recommendations, and so on that may impact your specific environment.

► **To create a dual port video group:**

1. Select Device Settings > Port Group Management. The Port Group Management page opens. Any existing port groups are displayed.
2. Click Add. The Port Group page opens, and all available ports are displayed in the Select Ports for Group section.

Note: If a port is already a part of blade server port group, another dual video port group, or 'standard' port group, the port is not an option since ports can only belong to a single port group at a time.

3. Select the Dual Video Port Group radio button.
4. From the Select Ports for Group section, click on the port you are designating as the primary port, then click Add to add it to the Selected text box. Be sure to add the primary port first.

*Note: Ideally, the permissions applied to each port in the port group should be the same. If they are not, the permissions of the port with the most restrictive permissions is applied to the port group. For example, if VM Access Deny is applied to one port and VM Access Read-Write is applied to another port, VM Access Deny is applied to the port group. See **Permissions and Dual Video Port Group Access** (on page 236) for information on how port permissions affect dual video port groups.*

5. Click on the port that you are designating as the secondary port and click Add to add it to the Selected text box.
6. Select the orientation of the page. The orientation you select depends on what works best with your monitor setup.
7. Click OK to create the port group.

Dual video port groups appear on the Port Access page as Dual Port types.

The primary and secondary ports that are a part of the port group appear on the Port Access page as Dual Port(P) and Dual Port(S), respectively. For example, if the CIM type is DCIM, "DCIM Dual Port (P)" is displayed.

Note: Dual Video port targets attached to a tier device should only be connected via the tier device, not through the tier base device.

Changing the Default GUI Language Setting

The KX III GUI defaults to English, but also supports the following localized languages:

- English (default)
- Japanese
- Simplified Chinese
- Traditional Chinese

► To change the GUI language:

1. Select Device Settings > Language. The Language Settings page opens.

2. From the Language drop-down, select the language you want to apply to the GUI.
3. Click Apply. Click Reset Defaults to change back to English.

Note: Once you apply a new language, the online help is also localized to match your language selection.

Security Management

Security Settings

From the Security Settings page, you can specify login limitations, user blocking, password rules, and encryption and share settings.

Raritan SSL certificates are used for public and private key exchanges, and provide an additional level of security. Raritan web server certificates are self-signed. Java applet certificates are signed by a VeriSign certificate. Encryption guarantees that your information is safe from eavesdropping and these certificates ensure that you can trust that the entity is Raritan, Inc.

► **To configure the security settings:**

1. Choose Security > Security Settings. The Security Settings page opens.
2. Update the **Login Limitations** (on page 188) settings as appropriate.
3. Update the **Strong Passwords** (on page 190) settings as appropriate.
4. Update the **User Blocking** (on page 191) settings as appropriate.
5. Update the Encryption & Share settings as appropriate.
6. Click OK.

► To reset back to defaults:

- Click Reset to Defaults.

Login Limitations

- ☐ Enable Single Login Limitation
- ☐ Enable Password Aging

Password Aging Interval (days)

60

- ☐ Log Out Idle Users

Idle Timeout (minutes)

30

Strong Passwords

- ☐ Enable Strong Passwords

Minimum length of strong password

8

Maximum length of strong password

16

- ☒ Enforce at least one lower case character
- ☒ Enforce at least one upper case character
- ☒ Enforce at least one numeric character
- ☒ Enforce at least one printable special character

Number of restricted passwords based on history

5

User Blocking

- ☒ Disabled
- ☐ Timer Lockout

Attempts

3

Lockout Time

5

- ☐ Deactivate User-ID

Failed Attempts

3

Encryption & Share

Encryption Mode

Auto

- ☒ Apply Encryption Mode to KVM and Virtual Media (Forced in FIPS 140-2 Mode)

- ☐ Enable FIPS 140-2 Mode (Changes are activated on reboot only!)

Current FIPS status: Inactive

PC Share Mode

Private

PC-Share Idle Timeout (seconds)

0

- ☐ VM Share Mode

Local Device Reset Mode

Enable Local Factory Reset

- ☒ Enable TLSv1.0

- ☒ Enable TLSv1.1

- ☒ Enable TLSv1.2

Login Limitations

Using login limitations, you can specify restrictions for single login, password aging, and the logging out idle users.

Limitation	Description
Enable single login limitation	When selected, only one login per user name is allowed at any time. When deselected, a given user name/password combination can be connected into the appliance from several client workstations simultaneously.
Enable password aging	When selected, all users are required to change their passwords periodically based on the number of days specified in Password Aging Interval field. This field is enabled and required when the Enable Password Aging checkbox is selected.

Limitation	Description
	Enter the number of days after which a password change is required. The default is 60 days.
Log out idle users, After (1-365 minutes)	Select the "Log off idle users" checkbox to automatically disconnect users after the amount of time you specify in the "After (1-365 minutes)" field. If there is no activity from the keyboard or mouse, all sessions and all resources are logged out. If a virtual media session is in progress, however, the session does not timeout. The After field is used to set the amount of time (in minutes) after which an idle user will be logged out. This field is enabled when the Log Out Idle Users option is selected. Up to 365 minutes can be entered as the field value

Login Limitations

☐ Enable Single Login Limitation

☐ Enable Password Aging

Password Aging Interval (days)

60

☒ Log Out Idle Users

Idle Timeout (minutes)

30

Strong Passwords

Strong passwords provide more secure local authentication for the system. Using strong passwords, you can specify the format of valid KX III local passwords such as minimum and maximum length, required characters, and password history retention.

Strong passwords require user-created passwords to have a minimum of 8 characters with at least one alphabetical character and one nonalphabetical character (punctuation character or number). In addition, the first four characters of the password and the user name cannot match.

When selected, strong password rules are enforced. Users with passwords not meeting strong password criteria will automatically be required to change their password on their next login. When deselected, only the standard format validation is enforced. When selected, the following fields are enabled and required:

Field	Description
Minimum length of strong password	Passwords must be at least 8 characters long. The default is 8, but administrators can change the minimum to 63 characters.
Maximum length of strong password	The default minimum length is 8, but administrators can set the maximum to a default of 16 characters. The maximum length of strong passwords is 63 characters.
Enforce at least one lower case character	When checked, at least one lower case character is required in the password.
Enforce at least one upper case character	When checked, at least one upper case character is required in the password.
Enforce at least one numeric character	When checked, at least one numeric character is required in the password.
Enforce at least one printable special character	When checked, at least one special character (printable) is required in the password.
Number of restricted passwords based on history	This field represents the password history depth. That is, the number of prior passwords that cannot be repeated. The range is 1-12 and the default is 5.

Strong Passwords

☐ Enable Strong Passwords

Minimum length of strong password

Maximum length of strong password

☒ Enforce at least one lower case character

☒ Enforce at least one upper case character

☒ Enforce at least one numeric character

☒ Enforce at least one printable special character

Number of restricted passwords based on history

User Blocking

The User Blocking options specify the criteria by which users are blocked from accessing the system after the specified number of unsuccessful login attempts.

The three options are mutually exclusive:

Option	Description
Disabled	The default option. Users are not blocked regardless of the number of times they fail authentication.

Option	Description
Timer Lockout	Users are denied access to the system for the specified amount of time after exceeding the specified number of unsuccessful login attempts. When selected, the following fields are enabled: ▪ Attempts - The number of unsuccessful login attempts after which the user will be locked out. The valid range is 1 - 10 and the default is 3 attempts. ▪ Lockout Time - The amount of time for which the user will be locked out. The valid range is 1 - 1440 minutes and the default is 5 minutes. <i>Note: Users in the role of Administrator are exempt from the timer lockout settings.</i>
Deactivate User-ID	When selected, this option specifies that the user will be locked out of the system after the number of failed login attempts specified in the Failed Attempts field: ▪ Failed Attempts - The number of unsuccessful login attempts after which the user's User-ID will be deactivated. This field is enabled when the Deactivate User-ID option is selected. The valid range is 1 - 10. When a user-ID is deactivated after the specified number of failed attempts, the administrator must change the user password and activate the user account by selecting the Active checkbox on the User page.

User Blocking

☒ Disabled

☐ Timer Lockout

Attempts
3

Lockout Time
5

☐ Deactivate User-ID

Failed Attempts
3

Encryption and Share

Using the Encryption & Share settings you can specify the type of encryption used, PC and VM share modes, and the type of reset performed when the KX III Reset button is pressed.

WARNING: If you select an encryption mode that is not supported by your browser, you will not be able to access the KX III from your browser.

Note that video performance may be impacted once encryption is applied. The extent of the performance impact varies based on the encryption mode.

For the best possible video performance and throughput, disable encryption mode to KVM and Virtual Media if your security policy permits this.

► To configure encryption and share:

1. Choose one of the options from the Encryption Mode drop-down list.
When an encryption mode is selected, a warning appears, stating that if your browser does not support the selected mode, you will not be able to connect to the KX III.
The warning states "When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the KX III."

Auto

This is the recommended option. The KX III autonegotiates to the highest level of encryption possible.

You must select Auto in order for the device and client to successfully negotiate the use of FIPS compliant algorithms.

AES-128

The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data. 128 is the key length. When AES-128 is specified, be certain that your browser supports it, otherwise you will not be able to connect. See *Checking Your Browser for AES Encryption* (on page 195) for more information.

AES-256

The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data. 256 is the key length. When AES-256 is specified, be certain that your browser supports it, otherwise you will not be able to connect. See *Checking Your Browser for AES Encryption* (on page 195) for more information.

Note: If you are running Windows XP® operating system with Service Pack 2, Internet Explorer® 7 cannot connect remotely to the KX III using AES-128 encryption.

For government and other high security environments, enable FIPS 140-2 Mode by selecting the Enable FIPS 140-2 checkbox. See *Enabling FIPS 140-2* (on page 196) for information on enabling FIPS 140-2.

1. PC Share Mode - Determines global concurrent remote KVM access, enabling up to eight remote users to simultaneously log into one KX III and concurrently view and control the same target server through the device. Click the drop-down list to select one of the following options:
 - Private - No PC share. This is the default mode. Each target server can be accessed exclusively by only one user at a time.
 - PC-Share - KVM target servers can be accessed by up to eight users (administrator or non-administrator) at one time. Each remote user has equal keyboard and mouse control, however, note that uneven control will occur if one user does not stop typing or moving the mouse. Selecting PC Share enables PC Share Timeout. Enter from 0 seconds to 600 seconds (10 minutes). The default timeout value is 0, so there is no exclusive keyboard/mouse control. If a user has not moved the mouse or entered keyboard input and the timeout period expires, the user relinquishes control, and another user can join.

2. If needed, select VM Share Mode. This option is enabled only when PC-Share mode is enabled. When selected, this option permits the sharing of virtual media and audio among multiple users, that is, several users can access the same virtual media or audio session. The default is disabled.
3. If needed, select Local Device Reset Mode. This option specifies which actions are taken when the hardware Reset button (at the back of the device) is depressed. For more information, see *Resetting the KX III Using the Reset Button* (see "Resetting the KX III Using the Reset Button on the Device" on page 397). Choose one of the following options:

Local device reset mode	Description
Enable Local Factory Reset (default)	Returns the KX III device to the factory defaults.
Enable Local Admin Password Reset	Resets the local administrator password only. The password is reset to raritan.
Disable All Local Resets	No reset action is taken.

Checking Your Browser for AES Encryption

If you do not know if your browser uses AES, check with the browser manufacturer or navigate to the <https://www.fortify.net/sslcheck.html> website using the browser with the encryption method you want to check. This website detects your browser's encryption method and displays a report.

AES 256-bit encryption is supported on the following web browsers:

- Firefox®
- Internet Explorer®
- Chrome®
- Safari®

In addition to browser support, AES 256-bit encryption requires the installation of Java™ Cryptography Extension® (JCE®) Unlimited Strength Jurisdiction Policy Files if you are using VKC/VKCS

Jurisdiction files for various JREs™ are available at the "other downloads" section the Java download website.

Enabling FIPS 140-2

For government and other high security environments, enabling FIPS 140-2 mode may be required.

The KX III uses an embedded FIPS 140-2-validated cryptographic module running on a Linux® platform per FIPS 140-2 Implementation Guidance section G.5 guidelines.

Once this mode is enabled, the private key used to generate the SSL certificates must be internally generated; it cannot be downloaded or exported.

Note that performance may be impacted once FIPS 140-2 mode is enabled.

► To enable FIPS 140-2:

1. Access the Security Settings page.
2. Enable FIPS 140-2 Mode by selecting the Enable FIPS 140-2 checkbox in the Encryption & Share section of the Security Settings page.

You will utilize FIPS 140-2 approved algorithms for external communications once in FIPS 140-2 mode.

The FIPS cryptographic module is used for encryption of session traffic consisting of video, keyboard, mouse, virtual media and smart card data.

3. Reboot the KX III. **Required**

Once FIPS mode is activated, 'FIPS Mode: Enabled' will be displayed in the Device Information section in the left panel of the screen.

For additional security, you can also create a new Certificate Signing Request once FIPS mode is activated. This will be created using the required key ciphers. Upload the certificate after it is signed or create a self-signed certificate. The SSL Certificate status will update from 'Not FIPS Mode Compliant' to 'FIPS Mode Compliant'.

When FIPS mode is activated, key files cannot be downloaded or uploaded. The most recently created CSR will be associated internally with the key file. Further, the SSL Certificate from the CA and its private key are not included in the full restore of the backed-up file. The key cannot be exported from KX III.

FIPS 140-2 Support Requirements

The KX III supports the use of FIPS 140-2 approved encryption algorithms. This allows an SSL server and client to successfully negotiate the cipher suite used for the encrypted session when a client is configured for FIPS 140-2 only mode.

Following are the recommendations for using FIPS 140-2 with the KX III:

KX III

- Set the Encryption & Share to Auto on the Security Settings page. See *Encryption & Share* (see "*Encryption and Share*" on page 193).

Microsoft Client

- FIPS 140-2 should be enabled on the client computer and in Internet Explorer.

▶ **To enable FIPS 140-2 on a Windows client:**

1. Select Control Panel > Administrative Tools > Local Security Policy to open the Local Security Settings dialog.
2. From the navigation tree, select Select Local Policies > Security Options.
3. Enable "System Cryptography: Use FIPS compliant algorithms for encryption, hashing and signing".
4. Reboot the client computer.

▶ **To enable FIPS 140-2 in Internet Explorer:**

1. In Internet Explorer, select Tools > Internet Options and click on the Advanced tab.
2. Select the Use TLS 1.0 checkbox.
3. Restart the browser.

Enabling TLS Protocols

To meet your security policies, enable the specific TLS protocol versions you require. Disabled protocols will not be used by the device.

▶ **To enable TLS protocols:**

1. Choose Security > Security Settings. In the Encryption and Share section, all TLS versions are listed.
2. Select the checkboxes of each TLS protocol version you want to enable. All versions are enabled by default. Unchecked protocols are not used. At least one protocol must be enabled.

Note: CommandCenter Secure Gateway only supports TLS v1.0. If you are using CC-SG, TLS v1.0 will be used to connect with KX III even if it is disabled here.

- Click OK to apply the settings.

Encryption & Share

Encryption Mode
 Auto ▼

☒ Apply Encryption Mode to KVM and Virtual Media (Forced in FIPS 140-2 Mode)

☐ Enable FIPS 140-2 Mode (Changes are activated on reboot only)

Current FIPS status: Inactive

PC Share Mode
 Private ▼

PC-Share Idle Timeout (seconds)
 0

☐ VM Share Mode

Local Device Reset Mode
 Enable Local Factory Reset ▼

☒ Enable TLSv1.0

☒ Enable TLSv1.1

☒ Enable TLSv1.2

Configuring IP Access Control

Using IP access control, you control access to your KX III. Note that IP access control restricts traffic of any kind from accessing the KX III, so NTP servers, RADIUS hosts, DNS hosts and so on must be granted access to the KX III.

By setting a global Access Control List (ACL) you are ensuring that your device does not respond to packets being sent from disallowed IP addresses. The IP access control is global, affecting the KX III as a whole, but you can also control access to your device at the group level. See ***Group-Based IP ACL (Access Control List)*** (on page 67) for more information about group-level control.

Important: IP address 127.0.0.1 is used by the KX III local port. When creating an IP Access Control list, 127.0.0.1 should not be within the range of IP addresses that are blocked or you will not have access to the KX III local port.

► To use IP access control:

- Select Security > IP Access Control to open the IP Access Control page.
- Select the Enable IP Access Control checkbox and the remaining fields on the page.
- Choose the Default Policy. This is the action taken for IP addresses that are not within the ranges you specify.
 - Accept - IP addresses are allowed access to the KX III device.

- Drop - IP addresses are denied access to the KX III device.

► **To add (append) rules:**

1. Type the IP address and subnet mask in the IPv4/Mask or IPv6/Prefix Length field.

Note: The IP address should be entered using CIDR (Classless Inter-Domain Routing notation, in which the first 24 bits are used as a network address).

2. Choose the Policy from the drop-down list.
3. Click Append. The rule is added to the bottom of the rules list.

► **To insert a rule:**

1. Type a rule #. A rule # is required when using the Insert command.
2. Type the IP address and subnet mask in the IPv4/Mask or IPv6/Prefix Length field.
3. Choose the Policy from the drop-down list.
4. Click Insert. If the rule # you just typed equals an existing rule #, the new rule is placed ahead of the exiting rule and all rules are moved down in the list.

Tip: The rule numbers allow you to have more control over the order in which the rules are created.

► **To replace a rule:**

1. Specify the rule # you want to replace.
2. Type the IP address and subnet mask in the IPv4/Mask or IPv6/Prefix Length field.
3. Choose the Policy from the drop-down list.
4. Click Replace. Your new rule replaces the original rule with the same rule #.

► **To delete a rule:**

1. Specify the rule # you want to delete.
2. Click Delete.

3. You are prompted to confirm the deletion. Click OK.

Home > Security > IP Access Control

IP Access Control

☒ Enable IP Access Control

Default policy
 ACCEPT 

Rule #	IPv4/Mask or IPv6/Prefix Length	Policy
1	192.168.59.192/32	ACCEPT
2	192.168.61.0/24	ACCEPT
3	255.255.0.0/16	ACCEPT

ACCEPT 

SSL and TLS Certificates

KX III uses the Transport Layer Security (TLS) for any encrypted network traffic between itself and a connected client.

When establishing a connection, KX III has to identify itself to a client using a cryptographic certificate.

KX III can generate a Certificate Signing Request (CSR) or a self-signed certificate using SHA-2.

The CA verifies the identity of the originator of the CSR.

The CA then returns a certificate containing its signature to the originator. The certificate, bearing the signature of the well-known CA, is used to vouch for the identity of the presenter of the certificate.

Important: Make sure your KX III date/time is set correctly.

When a self-signed certificate is created, the KX III date and time are used to calculate the validity period. If the KX III date and time are not accurate, the certificate's valid from - to date range may be incorrect, causing certificate validation to fail. See ***Configuring Date/Time Settings*** (on page 165).

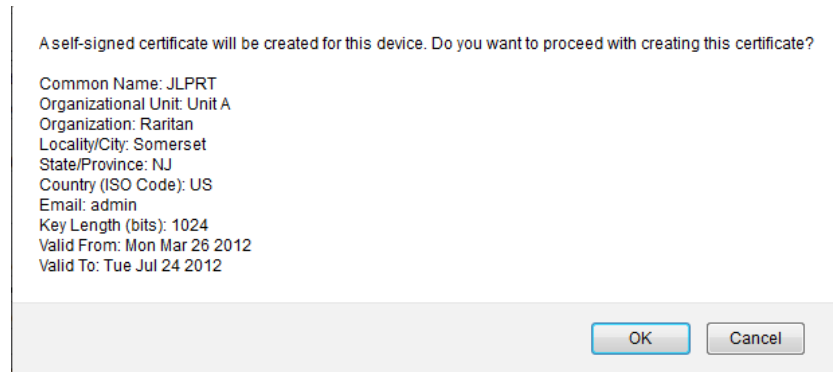
Note: The CSR must be generated on the KX III.

Note: When upgrading firmware, the active certificate and CSR are not replaced.

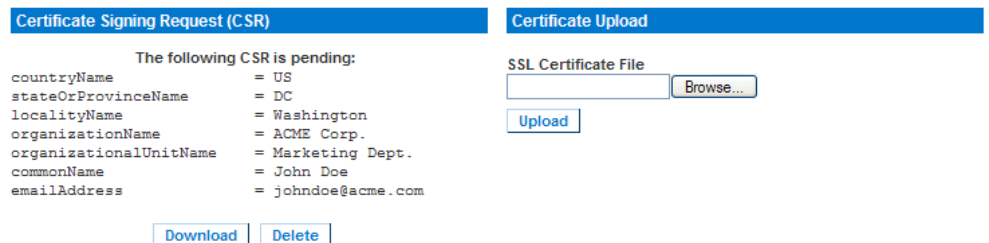
► **To create and install a SSL certificate:**

1. Select Security > Certificate.
2. Complete the following fields:
 - a. Common name - The network name of the KX III once it is installed on your network (usually the fully qualified domain name). The common name is identical to the name used to access the KX III with a web browser, but without the prefix "http://". In case the name given here and the actual network name differ, the browser displays a security warning when the KX III is accessed using HTTPS.
 - b. Organizational unit - This field is used for specifying to which department within an organization the KX III belongs.
 - c. Organization - The name of the organization to which the KX III belongs.
 - d. Locality/City - The city where the organization is located.
 - e. State/Province - The state or province where the organization is located.
 - f. Country (ISO code) - The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the U.S.
 - g. Email - The email address of a contact person that is responsible for the KX III and its security.
 - h. Subject Alternative Name (SAN) - Optional. Add up to ten SANs, which may include alternate hostnames. Maximum of 64 characters. This allows devices that are reachable under different names to pass the TLS hostname validation for each name registered in the TLS certificate. Enter the SAN in the Enter Hostname/IP address field, then click Add to create the list of SANs. Select a SAN and click Remove to delete.
 - i. Challenge Password - Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). Applicable when generating a CSR for CA Certification.

- j. Confirm Challenge Password - Confirmation of the Challenge Password. Applicable when generating a CSR for CA Certification.
- k. Key length - The length of the generated key in bits. 1024 is the default. Up to 4096 is supported.
- 3. To generate, do one of the following:
 - To generate self-signed certificate, do the following:
 - a. Select the Create a Self-Signed Certificate checkbox if you need to generate a self-signed certificate. When you select this option, the KX III generates the certificate based on your entries, and acts as the signing certificate authority. The CSR does not need to be exported and used to generate a signed certificate.
 - b. Specify the number of days for the validity range. Ensure the KX III date and time are correct. If the date and time are not correct, the certificate's valid date range may not be calculated correctly.
 - c. Click Create.
 - d. A confirmation dialog is displayed. Click OK to close it.



- e. Reboot the KX III to activate the self-signed certificate.
 - To generate a CSR to send to the CA for certification:
 - a. Click Create.
 - b. A message containing all of the information you entered appears.



- c. The CSR and the file containing the private key used when generating it can be downloaded by clicking Download CSR.
- d. Send the saved CSR to a CA for certification. You will get the new certificate from the CA.

Note: The CSR and the private key file are a matched set and should be treated accordingly. If the signed certificate is not matched with the private key used to generate the original CSR, the certificate will not be useful. This applies to uploading and downloading the CSR and private key files.

- Once you get the certificate from the CA, upload it to the KX III by clicking Upload.
- Reboot the KX III to activate the certificate.

After completing these steps the KX III has its own certificate that is used for identifying itself to its clients.

Important: If you destroy the CSR on the KX III there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described above. To avoid this, use the download function so you will have a copy of the CSR and its private key.

Security Banner

KX III provides you with the ability to add a security banner to the KX III login process. This feature requires users to either accept or decline a security agreement before they can access the KX III. The information provided in a security banner will be displayed in a Restricted Service Agreement dialog after users access KX III using their login credentials.

The security banner heading and wording can be customized, or the default text can be used. Additionally, the security banner can be configured to require that a user accepts the security agreement before they are able to access the KX III or it can just be displayed following the login process. If the accept or decline feature is enabled, the user's selection is logged in the audit log.

► To configure a security banner:

1. Click Security > Banner to open the Banner page.
2. Select Display Restricted Service Banner to enable the feature.
3. If you want to require users to acknowledge the banner prior to continuing the login process, select Require Acceptance of Restricted Service Banner. In order to acknowledge the banner, users will select a checkbox. If you do not enable this setting, the security banner will only be displayed after the user logs in and will not require users acknowledge it.

4. If needed, change the banner title. This information will be displayed to users as part of the banner. Up to 64 characters can be used.
5. Edit the information in the Restricted Services Banner Message text box. Up to 6000 characters can be entered or uploaded from a text file. To do this, do one of the following:
 - a. Edit the text by manually typing in the text box. Click OK.
 - b. Upload the information from .txt file by selecting the Restricted Services Banner File radio button and using the Browse feature to locate and upload the file. Click OK. Once the file is uploaded, the text from the file will appear in the Restricted Services Banner Message text box.

Note: You cannot upload a text file from the local port.

Home > Security > Banner

Banner

- ☒ Display Restricted Service Banner
- ☐ Require Acceptance of Restricted Service Banner

Banner Title

Restricted Access

☒ Restricted Service Banner Message:

Unauthorized access prohibited, all access and activities not explicitly authorized by management are unauthorized. All activities are monitored and logged. There is no privacy on this system. Unauthorized access and activities or any criminal activity will be reported to appropriate authorities.

☐ Restricted Service Banner File:

Browse...

OK Reset To Defaults Cancel

Maintenance

Audit Log

A log is created of KX III system events.

The audit log can contain up to approximately 2K worth of data before it starts overwriting the oldest entries.

To avoid losing audit log data, export the data to a syslog server or SNMP manager. Configure the syslog server or SNMP manager from the Device Settings > Event Management page. See ***Events Captured in the Audit Log and Syslog*** (on page 442) for information on what is captured in the audit log and syslog.

► **To view the audit log for your KX III:**

1. Choose Maintenance > Audit Log. The Audit Log page opens.
The Audit Log page displays events by date and time (most recent events listed first). The Audit Log provides the following information:
 - Date - The date and time that the event occurred based on a 24-hour clock.
 - Event - The event name as listed in the Event Management page.
 - Description - Detailed description of the event.

► **To save the audit log:**

Note: Saving the audit log is available only on the KX III Remote Console, not on the Local Console.

1. Click Save to File. A Save File dialog appears.
2. Choose the desired file name and location and click Save. The audit log is saved locally on your client machine with the name and location specified.

► **To page through the audit log:**

- Use the [Older] and [Newer] links.

Device Information

The Device Information page provides detailed information about your KX III device and the CIMs in use. This information is helpful should you need to contact Raritan Technical Support.

► **To view information about your KX III and CIMs:**

- Choose Maintenance > Device Information. The Device Information page opens.

The following information is provided about the KX III:

- Model
- Hardware Revision
- Firmware Version
- Serial Number
- MAC Address

The following information is provided about the CIMs in use:

- Port (number)
- Name
- Type of CIM - DCIM, PCIM, Rack PDU, VM, DVM-DP, DVM-HDMI, DVM-DVI
- Firmware Version
- Serial Number of the CIM - this number is pulled directly from the supported CIMs.
 - 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

Note: Only the numeric portion of the serial numbers are displayed for the DCIM-USB, DCIM-PS2 and DCIM-USB G2 CIMs. For example, XXX1234567 is displayed. The serial number prefix GN is displayed for CIMs that have field configured serial numbers.

Device Information	
Model:	DKX2-232
Hardware Revision:	0x48
Firmware Version:	2.4.0.3.399
Serial Number:	HKB7500230
MAC Address:	00:0d:5d:03:cc:b5

CIM Information

▲ Port	Name	Type	Firmware Version	Serial Number
5	SE-KX2-232-LP	PCIM	N/A	XXX9900169
6	Target Win XP	Dual-VM	3A86	PQ20304596
9	W2K3 Server	Dual-VM	3A86	PQ28350007
18	Win XP 2.4GHz P4 504MB	VM	2A7E	HUW7553560

Creating a KX III Backup and Restore File

From the Backup/Restore page, you can backup and restore the settings and configuration for your KX III.

In addition to using backup and restore for business continuity purposes, you can use this feature as a time-saving mechanism.

For instance, you can quickly provide access to your team from another KX III by backing up the user configuration settings from the KX III in use and restoring those configurations to the new KX III.

You can also set up one KX III and copy its configuration to multiple KX III appliances.

For KX II 2.5.0 and KX II 2.6.0 users, you are able to create a backup/restore file of a KX II's settings and apply them to a KX III. This can help you when you migrate to a KX III from a KX II. See ***Applying KX II Appliance Setting to a KX III Using a Backup/Restore File*** (see "Applying KX III Appliance Setting to a KX III Using a Backup/Restore File" on page 210)

Create a Backup File

Note: Backups are always complete system backups. Restores can be complete or partial depending on your selection.

► **If you are using Internet Explorer® 7 or later, to back up your KX III:**

1. Choose Maintenance > Backup/Restore. The Backup/Restore page opens.

Home > Maintenance > Backup / Restore

Backup / Restore

☒ Full Restore
☐ Protected Restore
☐ Custom Restore

☐ User and Group Restore
☐ Device Settings Restore

Restore File

2. Click Backup. A File Download dialog appears that contains an Open button. **Do not click Open.**

In IE 7 (and later), IE is used as the default application to open files, so you are prompted to open the file versus save the file. To avoid this, you must change the default application that is used to open files to WordPad®.

3. To do this:
 - a. Save the backup file. The backup file is saved locally on your client machine with the name and location specified.
 - b. Once saved, locate the file and right-click on it. Select properties.
 - c. In general tab, click Change and select WordPad.

Restore Your KX III Using a Restore File

WARNING: Exercise caution when restoring your KX III to an earlier version. Usernames and password in place at the time of the backup will be restored. If you do not remember the old administrative usernames and passwords, you will be locked out of the KX III.

In addition, if you used a different IP address at the time of the backup, that IP address will be restored as well. If the configuration uses DHCP, you may want to perform this operation only when you have access to the local port to check the IP address after the update.

Follow the steps here to apply a KX II backup/restore file to apply settings from the KX II to the KX III. Before proceeding, review the information in *Requirements to Apply a KX II Backup and Restore File to a KX III* (on page 210).

Note that some settings cannot be applied from a KX II to a KX III using the backup/restore function. See *KX II-to-KX III Unsupported Backup/Restore File Settings and Functions* (on page 211)

► To restore your KX III:

1. Choose Maintenance > Backup/Restore. The Backup/Restore page opens.

Home > Maintenance > Backup / Restore

Backup / Restore

☒ Full Restore
☐ Protected Restore
☐ Custom Restore
☐ User and Group Restore
☐ Device Settings Restore

Restore File

2. Choose the type of restore you want to run:
 - Full Restore - A complete restore of the entire system. Generally used for traditional backup and restore purposes.
 - Protected Restore - Everything is restored except appliance-specific information such as IP address, name, and so forth. With this option, you can setup one KX III and copy the configuration to multiple KX III appliances.
 - Custom Restore - With this option, you can select User and Group Restore, Device Settings Restore, or both:

- User and Group Restore - This option includes only user and group information. This option *does not* restore the certificate and the private key files. Use this option to quickly set up users on a different KX III.
 - Device Settings Restore - This option includes only appliance settings such as power associations, USB profiles, blade chassis related configuration parameters, and Port Group assignments. Use this option to quickly copy the appliance information.
3. Click Browse. A Choose File dialog appears.
 4. Navigate to and select the appropriate backup file and click Open. The selected file is listed in the Restore File field.
 5. Click Restore. The configuration is restored based on the type of restore selected, or the supported settings are applied from KX II.

Applying KX III Appliance Setting to a KX III Using a Backup/Restore File

You can create a backup/restore file of a KX III's settings, and then use it to apply the settings to a KX III.

Before restoring a file, review ***Requirements to Apply a KX II Backup and Restore File to a KX III*** (on page 210).

Some KX II settings and functions cannot be restored to a KX III. See ***KX II-to-KX III Unsupported Backup/Restore File Settings and Functions*** (on page 211).

For steps on creating a backup/restore file, see ***Create a Backup File*** (on page 208).

For steps on using a KX II file to apply settings to a KX III, follow the steps outlined in ***Restore Your KX III Using a Restore File*** (on page 209).

Requirements to Apply a KX II Backup and Restore File to a KX III

To apply settings from a KX II to a KX III using a KX II backup/restore file, the following conditions must be met:

- The KX II and KX III must be the same models.
For example -
 - You *can* apply settings to a KX3-432 from KX2-432
 - You *cannot* apply settings from KX2-464 to a KX3-432
- The KX II and KX III must be using the same CIMs (the CIM serial numbers must match) in order to apply the CIM settings to the KX III.

KX II-to-KX III Unsupported Backup/Restore File Settings and Functions

When you use a KX II backup/restore file to apply settings to a KX III, the following settings are *not* applied to the KX III.

- KX II Local Extended Port Settings (KX III does not support this feature)
- KX II video switching delay, resolution and refresh rates (these settings do not apply to KX III)
- KX II language setting
- You cannot use the backup and restore function to upgrade from KX II to KX III via CC-SG

USB Profile Management

From the USB Profile Management page, you can upload custom profiles provided by Raritan tech support. These profiles are designed to address the needs of your target server's configuration, in the event that the set of standard profiles does not already address them. Raritan tech support will provide the custom profile and work with you to verify the solution for your target server's specific needs.

► **To access the USB Profile Management page:**

- Choose Maintenance > USB Profile Management. The USB Profile Management page opens.

Home > Maintenance > USB Profile Management Logout

Profile successfully uploaded.

USB Profile File:

Selected	Active	Profile	Profile Key
☐	No	Dell Dimension 1 Custom Profile for Dell Dimension/n- Force full-speed is ON - Order: HID interface first, Mass Storage second - CDROM and removable drive cannot be used simultaneously	40000300

Deleting an active profile may be disruptive to sessions in progress.

► **To upload a custom profile to your KX III:**

1. Click Browse. A Choose File dialog appears.
2. Navigate to and select the appropriate custom profile file and click Open. The file selected is listed in the USB Profile File field.
3. Click Upload. The custom profile will be uploaded and displayed in the Profile table.

Note: If an error or warning is displayed during the upload process (for example, overwriting an existing custom profile), you may continue with the upload by clicking Upload or cancel it by clicking on Cancel.

► **To delete a custom profile to your KX III:**

1. Check the box corresponding to the row of the table containing the custom profile to be deleted.
2. Click Delete. The custom profile will be deleted and removed from the Profile table.

As noted, you may delete a custom profile from the system while it is still designated as an active profile. Doing so will terminate any virtual media sessions that were in place.

Handling Conflicts in Profile Names

A naming conflict between custom and standard USB profiles may occur when a firmware upgrade is performed. This may occur if a custom profile that has been created and incorporated into the list of standard profiles has the same name as a new USB profile that is downloaded as part of the firmware upgrade.

Should this occur, the preexisting custom profile will be tagged as 'old_'. For example, if a custom profile called GenericUSBProfile5 has been created and a profile with the same name is downloaded during a firmware upgrade, the existing file will then be called 'old_GenericUSBProfile5'.

You can delete the existing profile if needed. See **USB Profile Management** (on page 211) for more information.

Upgrading CIMs

Use this procedure to upgrade CIMs using the firmware versions stored in the memory of your KX III device. In general, all CIMs are upgraded when you upgrade the device firmware using the Firmware Upgrade page.

► **To upgrade CIMs using the KX III memory:**

1. Choose Maintenance > CIM Firmware Upgrade. The CIM Upgrade from page opens.
The Port (number), Name, Type, Current CIM Version, and Upgrade CIM Version are displayed for easy identification of the CIMs.
2. Check the Selected checkbox for each CIM you want to upgrade.
3. Click Upgrade. You are prompted to confirm the upgrade.

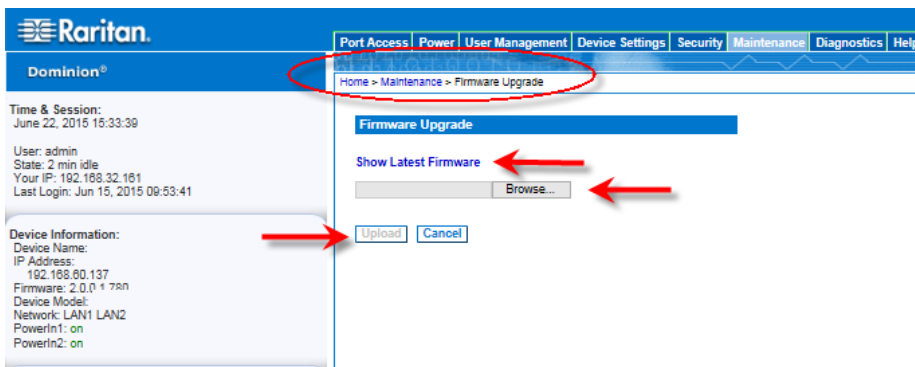
- Click OK to continue the upgrade. Progress bars are displayed during the upgrade. Upgrading takes approximately 2 minutes or less per CIM.

Upgrading the KX III Firmware

Use the Firmware Upgrade page to upgrade the firmware for your KX III and all attached CIMs. This page is available in the KX III Remote Console only.

Firmware Upgrade

Important: Do not turn off your KX III appliance or disconnect CIMs while the upgrade is in progress - doing so will likely result in damage to the appliance or CIMs.



► **To upgrade your KX III appliance:**

- Click the Show Latest Firmware link to locate the appropriate Raritan firmware distribution file (*.RFP) on the **Raritan website** <http://www.raritan.com> on the Firmware Upgrades web page.
- Unzip the file. Please read all instructions included in the firmware ZIP files carefully before upgrading.

Note: Copy the firmware update file to a local PC before uploading. Do not load the file from a network drive.

- Choose Maintenance > Firmware Upgrade. The Firmware Upgrade page opens.
- Click Browse to navigate to the directory where you unzipped the upgrade file.
- Click Upload from the Firmware Upgrade page.

Information about the upgrade and version numbers is displayed for your confirmation (if you opted to review CIM information, that information is displayed as well).

Note: At this point, connected users are logged out, and new login attempts are blocked.

6. Click Upgrade. Please wait for the upgrade to complete. Status information and progress bars are displayed during the upgrade. Upon completion of the upgrade, the appliance reboots (1 beep sounds to signal that the reboot has completed).
7. As prompted, close the browser and wait approximately 5 minutes before logging in to the KX III again.

Upgrade History

The KX III provides information about upgrades performed on the KX III and attached CIMS and DSAM units.

► **To view the upgrade history:**

- Choose Maintenance > Upgrade History. The Upgrade History page opens.

Information is provided about the KX III upgrade(s) that have been run, the final status of the upgrade, the start and end times, and the previous and current firmware versions. Information is also provided about the CIMS, which can be obtained by clicking the show link for an upgrade.

The CIM information provided is:

- Type - The type of CIM
- Port - The port where the CIM is connected
- User - The user who performed the upgrade
- IP - IP address firmware location
- Start Time - Start time of the upgrade
- End Time - end time of the upgrade
- Previous Version - Previous CIM firmware version
- Upgrade Version - Current CIM firmware version
- CIMS - Upgraded CIMS
- Result - The result of the upgrade (success or fail)

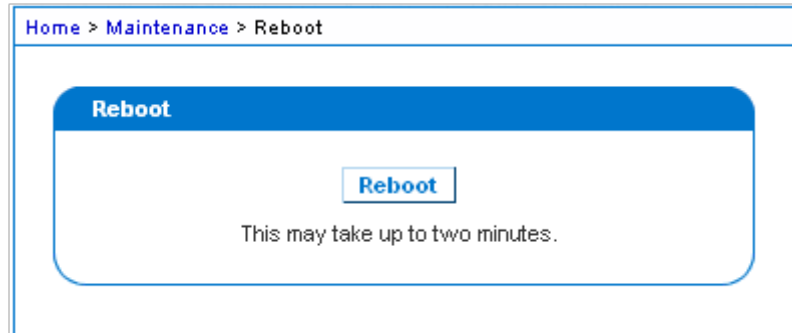
Rebooting the KX III

The Reboot page provides a safe and controlled way to reboot your KX III. This is the recommended method for rebooting.

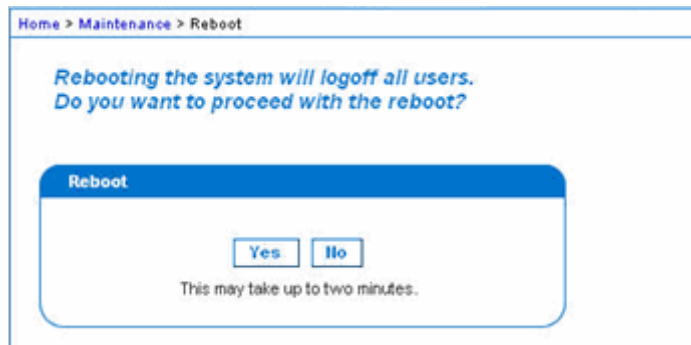
Important: All connections will be closed and all users will be logged off.

► **To reboot your KX III:**

1. Choose Maintenance > Reboot. The Reboot page opens.



2. Click Reboot. You are prompted to confirm the action. Click Yes to proceed with the reboot.



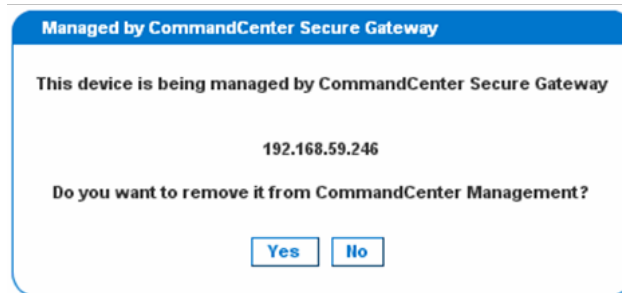
Stopping CC-SG Management

While KX III is under CC-SG management, if you try to access the device directly, you are notified that the device is under CC-SG management.

If you are managing KX III through CC-SG and connectivity between CC-SG and the KX III is lost after the specified timeout interval (typically 10 minutes), you are able to end the CC-SG management session from the KX III console.

Note: You must have the appropriate permissions to end CC-SG management of KX III.

1. Click Maintenance > Stop CC-SG Management. A message indicating that the device is being managed by CC-SG will be displayed. An option to remove the device from CC-SG management will also be displayed.



2. Click Yes to begin the process of removing the device from CC-SG management. A confirmation message displays.



3. Click Yes to remove the device CC-SG management. A confirmation message displays when CC-SG management has ended.



Diagnostics

Network Interface Page

The KX III provides information about the status of your network interface.

► **To view information about your network interface:**

- Choose Diagnostics > Network Interface. The Network Interface page opens.

The following information is displayed:

- Whether the Ethernet interface is up or down.
- Whether the gateway is pingable or not.
- The LAN port that is currently active.

► **To refresh this information:**

- Click Refresh.

Network Statistics Page

The KX III provides statistics about your network interface.

1. Choose Diagnostics > Network Statistics. The Network Statistics page opens.
2. Choose the appropriate option from the Options drop-down list.
3. Click Refresh. The relevant information is displayed in the Result field.

- Statistics - Produces a page similar to the one displayed here.

Home > Diagnostics > Network Statistics

Network Statistics

Options:
 --statistics ▼
 Refresh

Result:

```

Ip:
1897674 total packets received
0 forwarded
0 incoming packets discarded
1179770 incoming packets delivered
759937 requests sent out
1584 reassemblies required
264 packets reassembled ok
Icmp:
28027 ICMP messages received
0 input ICMP message failed.
ICMP input histogram:
destination unreachable: 4308
  
```

- Interfaces - Produces a page similar to the one displayed here.

Home > Diagnostics > Network Statistics

Network Statistics

Options:

Result:

```

Kernel Interface table
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0 1500 0 1821360 0 0 0 764900 0 0 0 ABMRU
eth1 1500 0 2438589 0 0 0 4 0 0 0 ABMRU
lo 16436 0 8131 0 0 0 8131 0 0 0 LRU
    
```

- Route - Produces a page similar to the one displayed here.

Home > Diagnostics > Network Statistics

Network Statistics

Options:

Result:

```

Kernel IPv6 routing table
Destination Next Hop Flags Metric Ref Use Iface
::1/128 :: U 0 0 1 lo
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
192.168.60.0 * 255.255.255.0 U 0 0 0 eth0
224.0.0.0 * 240.0.0.0 U 0 0 0 eth0
default 192.168.60.126 0.0.0.0 UG 0 0 0 eth0
    
```

Ping Host Page

Ping is a network tool used to test whether a particular host or IP address is reachable across an IP network. Using the Ping Host page, you can determine if a target server or another KX III is accessible.

1. Choose Diagnostics > Ping Host. The Ping Host page appears.
2. Type either the hostname or IP address into the IP Address/Host Name field.

Note: The host name cannot exceed 232 characters in length.

3. Click Ping. The results of the ping are displayed in the Result field.

4. Select the interface in the Network Interface drop-down box to ping on a specified interface. **Optional**

Home > Diagnostics > Ping Host

Ping Host

IP Address/Host Name:

Network Interface:

Result:

```

PING 192.168.80.137 (192.168.80.137): 68 data bytes
64 bytes from 192.168.80.137: seq=0 ttl=64 time=0.300 ms
64 bytes from 192.168.80.137: seq=1 ttl=64 time=0.139 ms
64 bytes from 192.168.80.137: seq=2 ttl=64 time=0.130 ms
64 bytes from 192.168.80.137: seq=3 ttl=64 time=0.150 ms

--- 192.168.80.137 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.130/0.179/0.300 ms
  
```

Note: In Isolation mode, choose to ping on Auto, LAN1 only, or LAN2 only.

Trace Route to Host Page

Trace route is a network tool used to determine the route taken to the provided hostname or IP address.

► To trace the route to the host:

1. Choose Diagnostics > Trace Route to Host. The Trace Route to Host page opens.
2. Type either the IP address or host name into the IP Address/Host Name field.

Note: The host name cannot exceed 232 characters in length.

3. Choose the maximum hops from the drop-down list (5 to 50 in increments of 5).
4. Click Trace Route. The trace route command is executed for the given hostname or IP address and the maximum hops. The output of trace route is displayed in the Result field.

5. Select the interface in the Network Interface drop-down box to trace route on a specified interface. **Optional**

Home > Diagnostics > Trace Route to Host

Trace Route to Host

IP Address/Host Name:

Network Interface:

Maximum Hops:

[Trace Route](#)

Result:

```

traceroute started wait for 2mins....
traceroute to 192.168.61.11 (192.168.61.11), 10 hops max, 38 byte packets
 1 192.168.60.5 (192.168.60.5) 2.222 ms 1.292 ms 2.269 ms
 2 192.168.60.5 (192.168.60.5) 2.149 ms !H *
 3 192.168.60.5 (192.168.60.5) 2.949 ms !H * 1.506 ms !H
            
```

Device Diagnostics

Note: This page is for use by Raritan Field Engineers or when you are directed by Raritan Technical Support.

Use this feature to download diagnostic information from the KX III to the client machine.

Two operations can be performed on this page:

- Execute a special diagnostics script provided by Raritan Technical Support during a critical error debugging session. The script is uploaded to the appliance and executed. Once this script has been executed, you can download the diagnostics messages using the Save to File function.
- Download the device diagnostic log for a snapshot of diagnostics messages from the KX III appliance to the client. This encrypted file is then sent to Raritan Technical Support. Only Raritan can interpret this file.

Note: This page is accessible only by users with administrative privileges.

1. Choose Diagnostics > KX III Diagnostics. The KX III Diagnostics page opens.

2. To execute a diagnostics script file emailed to you from Raritan Technical Support, retrieve the diagnostics file supplied by Raritan using the browse function.
3. Click Run Script. Send this file to Raritan Technical Support.
4. To create a diagnostics file to send to Raritan Technical Support, click Save to File and save the file locally from the Save As dialog.
5. Email this file as directed by Raritan Technical Support.

KX III Local Console - Administration Functions

The KX III provides at-the-rack access and administration via its local port. Access to KX III features are provided via the Local Console.

The majority of administrative functions performed from the KX III Remote Console are also performed from the Local Console.

This section is specific to Administrator tasks. For end user tasks performed from the Local Console, see ***KX III Local Console*** (on page 385).

Security and Authentication

In order to use the KX III Local Console, you must first authenticate with a valid username and password.

The KX III provides a fully-integrated authentication and security scheme, whether your access is via the network or the local port.

In either case, the KX III allows access only to those servers to which a user has access permissions. See ***User Management*** (on page 61) for additional information on specifying server access and security settings.

If your KX III has been configured for external authentication services (LDAP/LDAPS, RADIUS, or Active Directory), authentication attempts at the Local Console also are authenticated against the external authentication service.

Note: You can also specify no authentication for Local Console access; this option is recommended only for secure environments.

► To use the KX III Local Console:

1. Connect a keyboard, mouse, and video display to the local ports at the back of the KX III.
2. Start the KX III. The KX III Local Console interface displays.

Configuring KX III Local Port Settings from the Local Console

The standard local port can be configured from the Remote Console on the Port Configuration page, or from the Local Console on the Local Port Settings page.

From the Local Port Settings page, you can customize many settings for the KX III Local Console including keyboard, hot keys, video switching delay, power save mode, local user interface resolution settings, and local user authentication.

Note: Only users with administrative privileges can access these functions.

Note: Some changes you make to the settings on the Local Port Settings page restart the browser you are working in. If a browser restart occurs when a setting is changed, it is noted in the steps provided here.

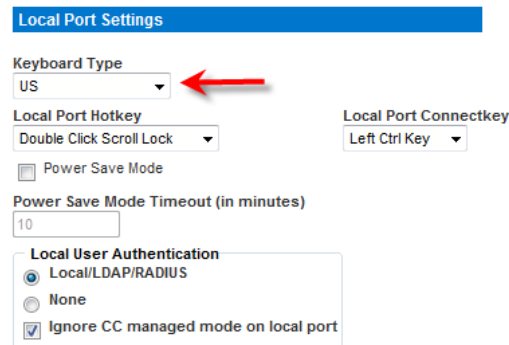
► To configure the local port settings:

1. Choose Device Settings > Local Port Settings. The Local Port Settings page opens.

Select the Local Console Keyboard Type

1. Choose the appropriate keyboard type from among the options in the drop-down list.

The browser will be restarted when this change is made.



The screenshot shows the 'Local Port Settings' page. At the top is a blue header bar with the text 'Local Port Settings'. Below this, there are several settings sections. The first section is 'Keyboard Type' with a dropdown menu currently set to 'US'. A red arrow points to this dropdown. Below it is the 'Local Port Hotkey' section with a dropdown set to 'Double Click Scroll Lock'. To the right of this is the 'Local Port Connectkey' section with a dropdown set to 'Left Ctrl Key'. Below these is a checkbox for 'Power Save Mode' which is unchecked. Underneath is a text input field for 'Power Save Mode Timeout (in minutes)' with the value '10'. The final section is 'Local User Authentication' with two radio buttons: 'Local/LDAP/RADIUS' (which is selected) and 'None'. Below the radio buttons is a checked checkbox for 'Ignore CC managed mode on local port'.

- US
- US/International
- United Kingdom
- French (France)
- German (Germany)
- German (Switzerland)
- Simplified Chinese
- Traditional Chinese
- Dubeolsik Hangul (Korean)
- JIS (Japanese Industry Standard)
- Portuguese (Portugal)
- Norwegian (Norway)
- Swedish (Sweden)
- Danish (Denmark)
- Belgian (Belgium)
- Hungarian
- Spanish
- Italian
- Slovenian

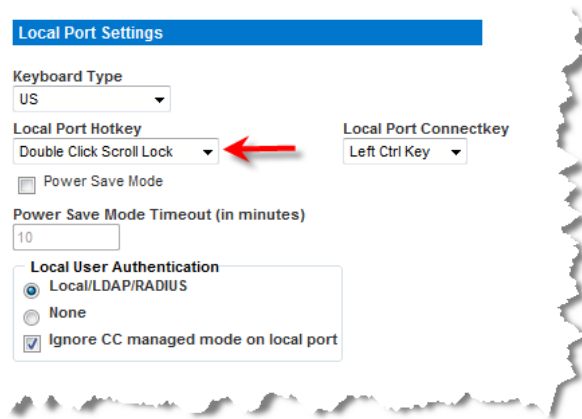
Note: Keyboard use for Chinese, Japanese, and Korean is for display only. Local language input is not supported at this time for KX III Local Console functions.

Note: If using a Turkish keyboard, you must connect to a target server through the Active KVM Client (AKC). It is not supported by other Raritan clients.

Select the Local Port Hotkey

1. Choose the local port hotkey. The local port hotkey is used to return to the KX III Local Console interface when a target server interface is being viewed. The default is to Double Click Scroll Lock, but you can select any key combination from the drop-down list:

Hot key:	Take this action:
Double Click Scroll Lock	Press Scroll Lock key twice quickly
Double Click Num Lock	Press Num Lock key twice quickly
Double Click Caps Lock	Press Caps Lock key twice quickly
Double Click Left Alt key	Press the left Alt key twice quickly
Double Click Left Shift key	Press the left Shift key twice quickly
Double Click Left Ctrl key	Press the left Ctrl key twice quickly



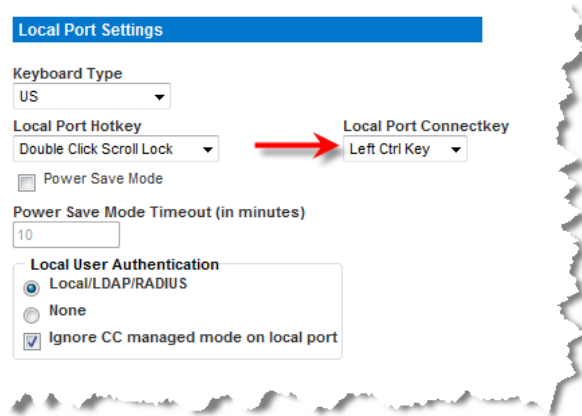
Select the Local Port Connect Key

Select the Local Port Connect key. Use a connect key sequence to connect to a target and switch to another target without returning to the GUI.

Then use the hot key to disconnect and return to the local port GUI

Once the local port connect key is created, it will appear in the Navigation panel of the GUI so you can use it as a reference. See ***Connect Key Examples*** (on page 387) for examples of connect key sequences.

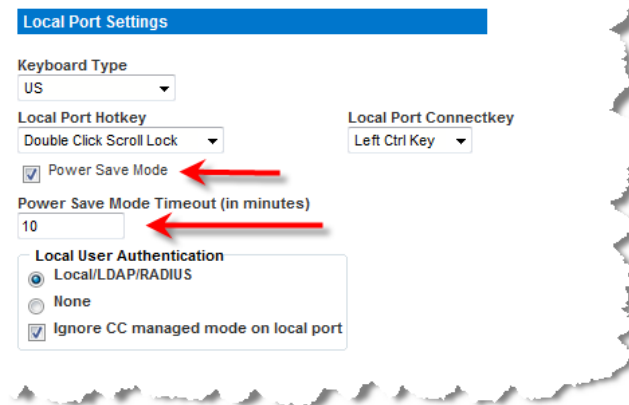
The connect key works for both standard servers and blade chassis.



Configure the Power Save Feature (Optional)

1. If you would like to use the power save feature:
 - a. Select the Power Save Mode checkbox.

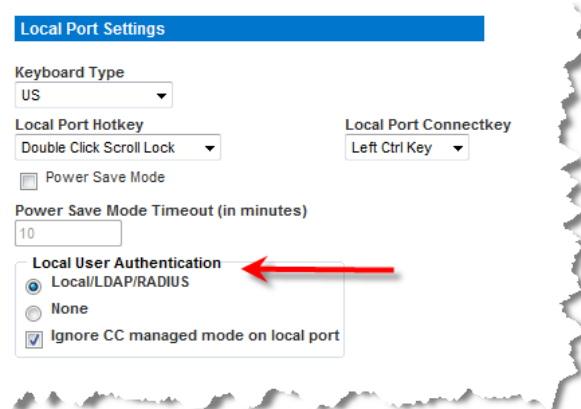
- b. Set the amount of time (in minutes) in which Power Save Mode will be initiated.



The screenshot shows the 'Local Port Settings' window. The 'Power Save Mode' checkbox is checked, and the 'Power Save Mode Timeout (in minutes)' is set to 10. Red arrows point to these two settings. The 'Local User Authentication' section shows 'Local/LDAP/RADIUS' selected with a radio button, and 'Ignore CC managed mode on local port' is checked.

Select the Local User Authentication

- Choose the type of local user authentication.
 - Local/LDAP/RADIUS. This is the recommended option.
 - None. There is no authentication for Local Console access. This option is recommended for secure environments only.



The screenshot shows the 'Local Port Settings' window. The 'Local User Authentication' section is highlighted with a red arrow pointing to the 'Local/LDAP/RADIUS' radio button. The 'Ignore CC managed mode on local port' checkbox is also checked.

Command Line Interface (CLI)

Overview

The Command Line Interface (CLI) can be used to configure the KX III network interface and perform diagnostic functions, provided you have the appropriate permissions to do so.

See **CLI Commands** (on page 230) for a list of all the commands, definitions and links to examples.

The following common commands can be used from all levels of the CLI to the preceding figure: top, history, logoff, quit, and help.

Accessing the KX III Using CLI

Access the KX III by using one of the following methods:

- SSH (Secure Shell) via IP connection

A number of SSH clients are available and can be obtained from the following locations:

- Putty - <http://www.chiark.greenend.org.uk/~sgtatham/putty/>
<http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- SSH Client from 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>

SSH Connection to the KX III

Use any SSH client that supports SSHv2 to connect to the KX III. You must enable SSH access from the Devices Services page.

Note: For security reasons, SSH V1 connections are not supported by the KX III.

SSH Access from a Windows PC

► **To open an SSH session from a Windows® PC:**

1. Launch the SSH client software.
2. Enter the IP address of the KX III server. For example, 192.168.0.192.
3. Choose SSH, which uses the default configuration port 22.
4. Click Open.

The login as: prompt appears.

See **Logging In** (on page 227).

SSH Access from a UNIX/Linux Workstation

► **To open an SSH session from a UNIX®/Linux® workstation:**

1. Log in as the user `admin`, enter the following command:
`ssh -l admin 192.168.30.222`

Enter your password when the `Password` prompt appears.

See *Logging In* (on page 227).

Logging In

► **To log in, enter the user name `admin` as shown:**

1. Log in as `admin`
2. The Password prompt appears. Enter the default password: `raritan`
 The welcome message displays. You are now logged on as an administrator.

After reviewing the following *Navigation of the CLI* (see "*Navigating the CLI*" on page 227) section, perform the Initial Configuration tasks.

Navigating the CLI

Before using the CLI, it is important to understand CLI navigation and syntax.

There are also some keystroke combinations that simplify CLI use.

Completion of Commands

The CLI supports the completion of partially-entered commands.

After entering the first few characters of an entry, press the Tab key.

- If the characters form a unique match, the CLI will complete the entry.
- If no match is found, the CLI displays the valid entries for that level.
- If multiple matches are found, the CLI displays all valid entries.

Enter additional text to make the entry unique and press the Tab key to complete the entry.

CLI Syntax -Tips and Shortcuts

Tips

- Commands are listed in alphabetical order.
- Commands are not case sensitive.
- Parameter names are a single word without an underscore.
- Commands without arguments default to show current settings for the command.
- Typing a question mark (?) after a command produces help for that command.
- A pipe symbol (|) indicates a choice within an optional or required set of keywords or arguments.

Shortcuts

- Press the Up arrow key to display the last entry.
- Press Backspace to delete the last character typed.
- Press Ctrl + C to terminate a command or cancel a command if you typed the wrong parameters.
- Press Enter to execute the command.
- Press Tab to complete a command. For example, `Admin Port >` `Conf` . The system then displays the `Admin Port > Config >` prompt.

Common Commands for All Command Line Interface Levels

Following are the commands that are available at all CLI levels. These commands also help navigate through the CLI.

Commands	Description
top	Return to the top level of the CLI hierarchy, or the “username” prompt.
history	Display the last 200 commands the user entered into the KX III CLI.
help	Display an overview of the CLI syntax.
quit	Places the user back one level.
logout	Logs out the user session.

Initial Configuration Using CLI

*Note: These steps, which use the CLI, are optional since the same configuration can be done via KVM. See **Getting Started** (see "Get Started Using KX III" on page 10) for more information.*

KX III devices come from the factory with default factory settings. When you first power up and connect to the device, you must set the following basic parameters so the device can be accessed securely from the network:

1. Reset the administrator password. All KX III devices are shipped with the same default password. Therefore, to avoid security breaches it is imperative that you change the admin password from raritan to one customized for the administrators who will manage the KX III device.
2. Assign the IP address, subnet mask, and gateway IP address to allow remote access.

Setting Parameters

To set parameters, you must be logged on with administrative privileges.

Setting Network Parameters

Network parameters are configured using the interface command.

```
admin > Config > Network > interface ipauto none ip  
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1 mode  
auto
```

When the command is accepted, the device automatically drops the connection. You must reconnect to the device using the new IP address and the user name and password you created in the resetting factory default password section.

Important: If the password is forgotten, the KX III will need to be reset to the factory default from the Reset button on the back of the KX III. The initial configuration tasks will need to be performed again if this is done.

The KX III now has the basic configuration and can be accessed remotely via SSH, GUI, or locally using the local serial port. The administrator needs to configure the users and groups, services, security, and serial ports to which the serial targets are attached to the KX III.

CLI Prompts

The Command Line Interface prompt indicates the current command level.

The root portion of the prompt is the login name.

`admin` is the root portion of a command when you establish a direct admin serial port connection via a terminal emulation application.

admin >

CLI Commands

- Enter `admin > help`.

Command	Description
config	Change to config sub menu.
diagnostics	Change to diag sub menu.
help	Display overview of commands.
history	Display the current session's command line history.
listports	List accessible ports.
logout	Logout of the current CLI session.
top	Return to the root menu.
userlist	List active user sessions.

- Enter `admin > config > network`.

Command	Description
dns	Display DNS information
ethernetfailover	Enable or disable automatic failover

Command	Description
help	Display overview of commands.
history	Display the current session's command line history.
interface	Set/get network parameters.
ipv6_interface	Set/get IPv6 network parameters.
logout	Logout of the current CLI session.
name	Device name configuration.
quit	Return to previous menu.
top	Return to the root menu.

Security Issues

Elements to consider when addressing security for console servers:

- Encrypting the data traffic sent between the operator console and KX III.
- Providing authentication and authorization for users.
- Security profile.

The KX III supports each of these elements; however, they must be configured prior to general use.

Administering the KX III Console Server Configuration Commands

Note: CLI commands are the same for SSH and Local Port access sessions.

The Network command can be accessed in the Configuration menu for the KX III.

Configuring Network

The network menu commands are used to configure the KX III network adapter.

Commands	Description
interface	Configure the KX III network interface.
name	Network name configuration

Commands	Description
ipv6_interface	Set/get IPv6 network parameters.
dns	
ethernetfailover	

Interface Command

The Interface command is used to configure the KX III network interface. The syntax of the interface command is:

```
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> IP Address
mask <subnetmask> Subnet Mask
gw <ipaddress> Gateway IP Address
mode <mode> Set Ethernet Mode
(auto/10hdx/10fdx/100hdx/100fdx/1000fdx)
```

Interface Command Example

The following command enables the interface number 1, sets the IP address, mask, and gateway addresses, and sets the mode to auto detect.

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

Name Command

The name command is used to configure the Device Name and preferred hostname. The syntax of the name is:

```
name [devicename <devicename>] [hostname <hostname>]
```

Device name configuration

```
devicename <devicename>    Device Name
hostname  <hostname>      Preferred host name (DHCP
only)
```

Name Command Example

The following command sets the device name:

```
Admin > Config > Network > name devicename My-KSX2
```

IPv6 Command

Use the IPv6_interface command to set IPv6 network parameters and retrieve existing IPv6 parameters.

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

Dual Video Port Groups

Servers with dual video cards can be remotely accessed with an extended desktop configuration, which is available to remote users. This is done by creating dual port video groups.

Extended desktop configurations allow you to view the target server desktop across two monitors vs. the standard single monitor view.

Once a dual port video group is selected, all port channels in that group open simultaneously.

See ***Dual Port Video Configuration Steps*** (on page 238)

Review the information in this section for important information regarding dual port video groups.

Note: Dual port video groups are not supported by models with only one KVM channel such as KX3-108 and KX3-116 models.

Recommendations for Dual Port Video

Set the target server's primary and secondary displays to the same video resolution in order to maintain mouse synchronization and minimize having to periodically resync.

Depending on the desired orientation, the top display (vertical orientation) or left display (horizontal orientation) should be the designated primary display. This display will provide active menu selection for virtual media, audio, smart card and mouse operations.

In order to provide intuitive mouse movement and control, the following should have the same display orientation:

- Client PC's primary and secondary displays
- Raritan device's dual video port group configuration
- Target server's primary and secondary displays

Only the following Client Launch Settings will be applied to dual port video displays:

- Select standard display or full screen Window mode when launching KVM client
- Enable video scaling
- Enable pinning menu toolbar when in full screen mode

The use of single mouse mode is not recommended when displaying dual video ports in full screen mode on a single client monitor. This will require exiting single mouse mode in order to access and view the other display.

Dual Video Port Group Supported Mouse Modes

Target operating systems	Supported mouse modes	Comments
All Windows® operating systems	Intelligent, Standard and Single Mouse Modes	If 'Stretch' mode is supported by the target server video card, Absolute mouse mode operates correctly. Stretch mode means the target server manages the dual display as a single, contiguous, virtual display. In contrast, the target server considers the displays as two independent displays when configured in Extended mode.

Target operating systems	Supported mouse modes	Comments
		For Extended mode, Intelligent Mouse mode is recommended.
Linux®	Intelligent and Standard Mouse Modes	Linux® users may experience display and mouse movement issues using single mouse mode. Raritan recommends Linux users do not use Single Mouse mode.
Mac® operating system	Single Mouse Mode	For Mac targets with multiple monitors, use a standard mouse in Single-Cursor mode.

CIMs Required for Dual Video Support

The following CIMs support the dual video port feature:

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-DP
- D2CIM-DVUSB-HDMI
- DCIM-USBG2

Review Digital CIM Target Server Timing and Video Resolution for important information regarding digital CIMs. See ***Supported Computer Interface Module (CIMs) Specifications*** (on page 421) for CIM specifications.

If the original CIM attached to a primary or secondary video port is disconnected and replaced with another CIM, the port is removed from the dual port video group. If needed, re-add the port to the group.

Note: The CIM you use depends on your target server requirements.

Dual Port Video Group Usability Notes

Following are various functions that are affected when using the dual port video group feature.

- Client Launch Settings that are configured in the VKC, VKCS, and AKC clients via Tools > Options > Client Launch Settings will be applied to dual video port groups as follows:
 - Window Mode settings will be applied

- Monitor settings will NOT be applied. Instead the Port Group Management configured 'Display Orientation' will be applied.
- Other - Enable Single Mouse Cursor setting will NOT be applied
- Other - Enable Scale Video setting will be applied
- Other - Pin Menu Toolbar setting will be applied
- Dragging and moving items between windows on the primary and secondary target requires a release and press of the mouse button as the item is moved from one window to the other.
- On Linux® and Mac® target servers, when Caps Scroll, and Num Lock is turned on, the Caps Lock indicator in the status bar of the primary port window is displayed, but the indicator may not be displayed in the status bar of the secondary port window.

Permissions and Dual Video Port Group Access

Ideally, the permissions applied to each port in the port group should be the same. If they are not, the permissions of the port with the most restrictive permissions are applied to the port group.

For example, if VM Access Deny is applied to one port and VM Access Read-Write is applied to another port, VM Access Deny is applied to the port group.

If a user does not have the appropriate permissions to access a port that is part of a dual video port group, only the port that they do have permissions to access is displayed. If a user does not have permissions to access either port, access is denied.

A message indicating that the port is either not available or the user does not have permission to access the port is displayed when they try to access it.

Example Dual Port Video Group Configuration

The following is a general example.

Your configuration may vary in the type of CIMs used, the port you designate as the primary port, the ports you are connecting to and so on.

In this example, we are using:

- A target server with two video ports
- Target server video port 1 as the primary port, and target server video port 2 as the secondary port
- A KX3-832 appliance
- A D2CIM-DVUSB-DP CIMs
- A target server and remote client running the Microsoft® Windows 7® operating system
- Intelligent mouse mode

An extended desktop view on the target server and remote client, so we are configuring the KX III to support a "Horizontal - Primary (Left), Secondary (Right)" display orientation.

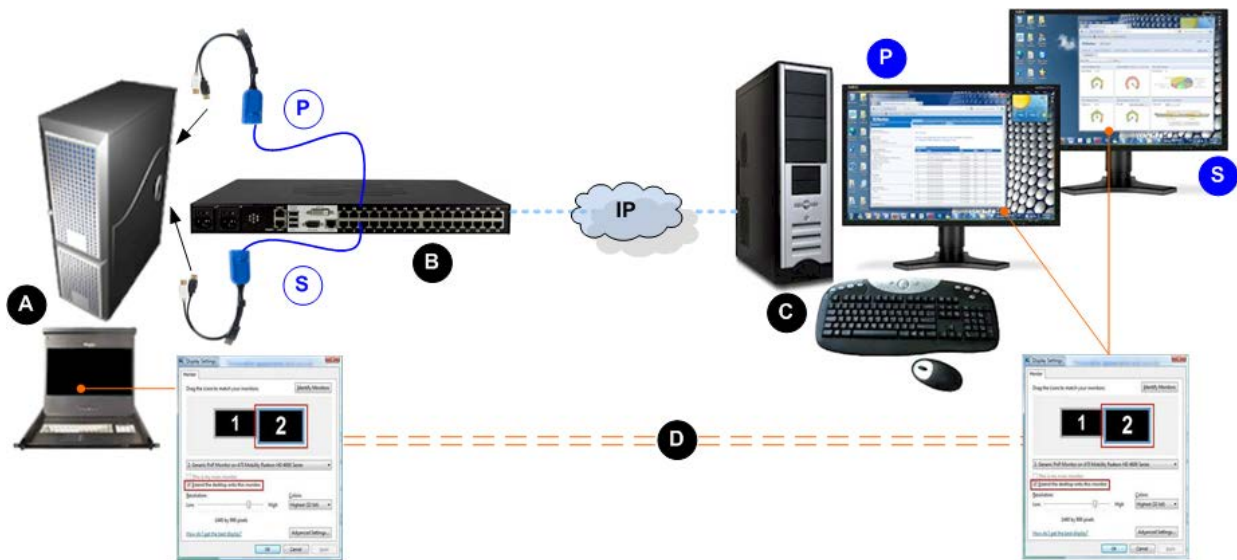


Diagram key	
A	Remote client - configure the dual port video group and display settings
B	KX III

Diagram key	
	Connection from the target's primary (first) video port to the KX III
	Connection from the target's secondary (second) video port to the KX III
IP connection between the KX III and remote client	
	Target server - configure the display settings and launch the dual port video group
	Display settings are the same on the remote client and target server (recommended)
	Horizontal - Primary (Left) - defined on the Port Group Management page in KX III
	Secondary (Right) - defined on the Port Group Management page in KX III

Dual Port Video Configuration Steps

Step 1: Configure the Target Server Display

For information on display orientations and mouse modes, review the previous topics in this section.

Note: See your target server or operating system user documentation for exact steps on configuring display settings.

► To configure target server display and mouse settings:

1. At the target server, configure the target server display orientation for each video port to match the display orientation of your remote client.

For example, if you are using an extended desktop orientation moving from left-to-right across two monitors at the remote client, set the target server display orientation to the same.
2. Ensure that your target server's video has already been set to a supported resolution and refresh rate. See ***KX III Supported Target Server Video Resolutions*** (on page 419)

Step 2: Connect the Target Server to the KX III

Dual port video groups can be created from existing port connections, or new port connections.

The steps provided here assume you are creating new connections.

If you are creating a dual port video group from existing connections, see **Step 4: Create the Dual Video Port Group** (on page 240).

► **To connect the equipment:**

1. Install and power up your target server per the manufacturer's instructions if you have not already done so.
2. Attach each CIM's video connector to each of the target's video output ports, then connect the USB cables to available USB ports on the target.
3. Connect each CIM to the Raritan device using a CAT5/6 cable.
4. If you have not already done so:
 - a. Connect the Raritan device to an AC power source using the provided power cable
 - b. Connect to the Raritan device network port and local port (if needed)
 - c. Configure the Raritan device.
5. Launch a supported web browser.
6. Enter the URL that corresponds to the client you want to use:
 - `http://IP-ADDRESS` launches the Active KVM Client from supported Microsoft .Net based environments or launches the Virtual KVM Client
 - Or
 - `http://IP-ADDRESS/vkc` for the Java-based Virtual KVM Client. Firefox 42 and later and Chrome 45 and later are not supported. Use VKCS with these browsers.
 - Or
 - `http://IP-ADDRESS/vkcs` for the standalone Java-based Virtual KVM Client for Chrome, Firefox, Edge, and Internet Explorer 11 browsers.
 - Or
 - `http://IP-ADDRESS/admin` for an administration-only client without target access capability. This client does not require .NET or Java.

IP-ADDRESS is the IP address assigned to your KX III

You can also use HTTPS, or the DNS name of the KX III assigned by your administrator (if applicable).

You are always redirected to the IP address from HTTP to HTTPS.

7. Enter your username and password, then click Login.
8. Accept the user agreement (if applicable).
9. If security warnings appear, accept and/or allow access.

Step 3: Configure the Mouse Mode and Ports

Once you have connected the target server to the Raritan device through the target server video ports, it detects the connection and displays the ports on the Port Configuration page.

For instructions, see **Configuring Standard Target Servers** (on page 99)

After the ports are configured, they can be grouped in a dual video port group.

*Note: Existing ports do not have to be configured if you have already done so when creating dual port video groups. See **Creating a Dual Video Port Group** (on page 185)*

Configure the target server mouse mode after you connect to the target. See **Dual Video Port Group Supported Mouse Modes** (on page 234)

Step 4: Create the Dual Video Port Group

See **Creating a Dual Video Port Group** (on page 185)

Step 5: Launch a Dual Port Video Group

Once you have created the dual video port group, it is available on the Port Access page.

You cannot remotely connect to the dual video port group by clicking on a primary port unless two KVM channels are available. If two channels are not available, the Connect link is not displayed.

Session timeouts that are configured on the KX III are applied to both ports of a dual video group.

► **To launch a dual port group:**

- On the Port Access page, click on the primary port name, then click Connect.

Both connections are launched at once and displayed in two different windows.

Once the windows are displayed, they can be moved based on the display setup you are using. For example, if you are using extended desktop mode, the port windows can be moved between monitors.



Raritan Client Navigation when Using Dual Video Port Groups

When using full screen mode in the clients, switch between ports by:

- Virtual KVM Client (VKC)
 - Pressing Alt+Tab
 - For Mac® clients, pressing F3, then selecting the port display
- Active KVM Client (AKC)
 - Clicking your mouse outside the display window, then pressing Alt+Tab
- HKC
 - See *HTML KVM Client (HKC) Help* (on page 305).

Direct Port Access and Dual Port Video Groups

Direct Port Access allows users to bypass having to use the KX III's Login dialog and Port Access page.

This feature also provides the ability to enter a username and password directly to proceed to the target, if the username and password is not contained in the URL.

If you are accessing a target that is part of a dual port video group, direct port access uses the primary port to launch both the primary and secondary ports.

Direct port connections to the secondary port are denied, and usual permission rules apply.

For information on the dual port video group feature, see **Creating a Dual Video Port Group** (on page 185).

For information on direct port access, see **Enabling Direct Port Access via URL** (on page 149).

Dual Port Video Groups Displayed on the Ports Page

Note: The dual video primary port is defined when the port group is created.

Note: You cannot remotely connect to the dual video port group by clicking on a primary port unless two KVM channels are available. If two channels are not available, the Connect link is not displayed.

For dual video port groups, the primary port is included in a port scan, but the secondary port is not included when connecting from a remote client. Both ports can be included in the scan from the Local Port.

See Working with Target Servers for more information on what is displayed on the Ports page, and see **Scanning Ports** (see "**Scanning Ports - Remote Console**" on page 375) for information on performing scans.

Chapter 4 Virtual Media

In This Chapter

Overview	243
Prerequisites for Using Virtual Media	244
Mounting Local Drives	245
Supported Tasks Via Virtual Media	245
Supported Virtual Media Types	246
Supported Virtual Media Operating Systems	246
Number of Supported Virtual Media Drives	247
Connecting and Disconnecting from Virtual Media.....	247
Virtual Media in a Windows XP Environment.....	249
Virtual Media in a Linux Environment.....	250
Virtual Media in a Mac Environment	252
Virtual Media File Server Setup (File Server ISO Images Only).....	253

Overview

All KX III models support virtual media. Virtual media extends KVM capabilities by enabling target servers to remotely access media from a client PC and network file servers.

With this feature, media mounted on client PCs and network file servers are essentially "mounted virtually" by the target server. The target server can then read from and write to that media as if it were physically connected to the target server itself.

Each KX III comes equipped with virtual media to enable remote management tasks using the widest variety of CD, DVD, USB, audio playback and record devices, internal and remote drives, and images.

Virtual media sessions are secured using 128 or 256 bit AES encryption.

Prerequisites for Using Virtual Media

KX III Virtual Media Prerequisites

- For users requiring access to virtual media, the KX III permissions must be set to allow access to the relevant ports, as well as virtual media access (VM Access port permission) for those ports. Port permissions are set at the group-level.
- A USB connection must exist between the device and the target server.
- If you want to use PC-Share, Security Settings must also be enabled in the Security Settings page. **Optional**
- You must choose the correct USB profile for the KVM target server you are connecting to.

Remote PC VM Prerequisites

- Certain virtual media options require administrative privileges on the remote PC (for example, drive redirection of complete drives).

Note: If you are using Microsoft Vista or Windows 7, disable User Account Control or select Run as Administrator when starting Internet Explorer. To do this, click the Start Menu, locate IE, right-click and select Run as Administrator.

Target Server VM Prerequisites

- KVM target servers must support USB connected drives.
- USB 2.0 ports are faster and preferred.

CIMs Required for Virtual Media

You must use one of the following CIMs is to use virtual media:

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

The black USB connector on the DVUSB CIMs are used for the keyboard and mouse. The gray connector is used for virtual media.

Keep both USB plugs of the CIM connected to the device.

The device may not operate properly if both plugs are not connected to the target server.

Mounting Local Drives

This option mounts an entire drive, which means the entire disk drive is mounted virtually onto the target server.

Use this option for hard drives and external drives only. It does not include network drives, CD-ROM, or DVD-ROM drives.

Notes on Mounting Local Drives

KVM target servers running the Windows XP® operating system may not accept new mass storage connections after an NTFS-formatted partition (for example, the local C drive) has been redirected to them.

If this occurs, close the Remote Console and reconnect before redirecting another virtual media device. If other users are connected to the same target server, they must also close their connections to the target server.

Supported Tasks Via Virtual Media

Virtual media provides the ability to perform tasks remotely, such as:

- Transferring files
- Running diagnostics
- Installing or patching applications
- Complete installation of the operating system
- Record and playback of digital audio

Important: Once you are connected to a virtual media drive, do not change mouse modes in the KVM client if you are performing file transfers, upgrades, installations or other similar actions. Doing so may cause errors on the virtual media drive or cause the virtual media drive to fail.

Supported Virtual Media Types

The following virtual media types are supported for Windows®, Mac® and Linux™ clients:

- Internal and external hard drives
- Internal and USB-mounted CD and DVD drives
- USB mass storage devices
- PC hard drives
- ISO images (disk images)

ISO9660 is the standard supported by Raritan. However, other ISO standards can be used.

- Digital audio devices*

Conditions when Read/Write is Not Available

Virtual media Read/Write is not available in the following situations:

- For Linux® and Mac® clients
- When the drive is write-protected
- When the user does not have Read/Write permission:
 - Port Permission Access is set to None or View
 - Port Permission VM Access is set to Read-Only or Deny

Supported Virtual Media Operating Systems

The following client operating systems are supported:

- Windows® 7 operating system
- Windows 8 operating system
- Windows XP® operating system
- openSUSE® 11.4 Celadon (x86_64)
- Fedora® 18
- RHEL® 6.4
- OSX Mountain Lion® 10.7 (and later)
- Solaris® 10

The Active KVM Client (AKC) can be used to mount virtual media types but only for Windows operating systems.

Number of Supported Virtual Media Drives

With the virtual media feature, you can mount up to two drives (of different types) that are supported by the USB profile currently applied to the target. These drives are accessible for the duration of the KVM session.

For example, you can mount a specific CD-ROM, use it, and then disconnect it when you are done. The CD-ROM virtual media “channel” will remain open, however, so that you can virtually mount another CD-ROM. These virtual media “channels” remain open until the KVM session is closed as long as the USB profile supports it.

To use virtual media, connect/attach the media to the client or network file server that you want to access from the target server.

This need not be the first step, but it must be done prior to attempting to access this media.

Connecting and Disconnecting from Virtual Media

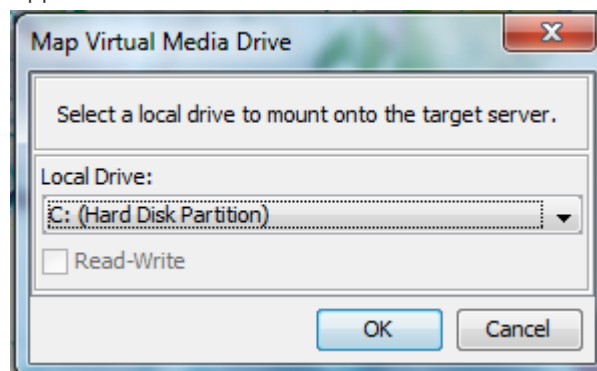
Access a Virtual Media Drive on a Client Computer

Important: Once you are connected to a virtual media drive, do not change mouse modes in the KVM client if you are performing file transfers, upgrades, installations or other similar actions. Doing so may cause errors on the virtual media drive or cause the virtual media drive to fail.

► **To access a virtual media drive on the client computer:**

1. From the KVM client, choose Virtual Media > Connect Drive, or click

the Connect Drive... button . The Map Virtual Media Drive dialog appears.



2. Choose the drive from the Local Drive drop-down list.

If you want Read and Write capabilities, select the Read-Write checkbox.

This option is disabled for nonremovable drives. See the ***Conditions when Read/Write is Not Available*** (on page 246) for more information.

When checked, you will be able to read or write to the connected USB disk.

WARNING: Enabling Read/Write access can be dangerous! Simultaneous access to the same drive from more than one entity can result in data corruption. If you do not require Write access, leave this option unselected.

3. Click OK. The media will be mounted on the target server virtually. You can access the media just like any other drive.

Mounting CD-ROM/DVD-ROM/ISO Images

This option mounts CD-ROM, DVD-ROM, and ISO images.

Note: ISO9660 format is the standard supported by Raritan. However, other CD-ROM extensions may also work.

► **To access a CD-ROM, DVD-ROM, or ISO image:**

1. From the KVM client, choose Virtual Media > Connect CD-ROM/ISO Image, or click the Connect CD ROM/ISO button . The Map Virtual Media CD/ISO Image dialog appears.
2. For internal and external CD-ROM or DVD-ROM drives:
 - a. Choose the Local CD/DVD Drive option.
 - b. Choose the drive from the Local CD/DVD Drive drop-down list. All available internal and external CD and DVD drive names will be populated in the drop-down list.
 - c. Click Connect.
3. For ISO images:
 - a. Choose the ISO Image option. Use this option when you want to access a disk image of a CD, DVD, or hard drive. ISO format is the only format supported.
 - b. Click Browse.
 - c. Navigate to the path containing the disk image you want to use and click Open. The path is populated in the Image Path field.
 - d. Click Connect.
4. For remote ISO images on a file server:
 - a. Choose the Remote Server ISO Image option.

- b. Choose Hostname and Image from the drop-down list. The file servers and image paths available are those that you configured using the File Server Setup page. Only items you configured using the File Server Setup page will be in the drop-down list.
- c. File Server Username - User name required for access to the file server. The name can include the domain name such as mydomain/username.
- d. File Server Password - Password required for access to the file server (field is masked as you type).
- e. Click Connect.

The media will be mounted on the target server virtually. You can access the media just like any other drive.

Note: If you are working with files on a Linux® target, use the Linux Sync command after the files are copied using virtual media in order to view the copied files. Files may not appear until a sync is performed.

Note: If you are using the Windows 7® operating system®, Removable Disk is not displayed by default in the Window's My Computer folder when you mount a Local CD/DVD Drive or Local or Remote ISO Image. To view the Local CD/DVD Drive or Local or Remote ISO Image in this folder, select Tools > Folder Options > View and deselect "Hide empty drives in the Computer folder".

Note: You cannot access a remote ISO image via virtual media using an IPv6 address due to third-party software technical limitations.

Disconnect from Virtual Media Drives

► To disconnect the virtual media drives:

- For local drives, choose Virtual Media > Disconnect Drive.
- For CD-ROM, DVD-ROM, and ISO images, choose Virtual Media > Disconnect CD-ROM/ISO Image.

Note: In addition to disconnecting the virtual media using the Disconnect command, simply closing the KVM connection closes the virtual media as well.

Virtual Media in a Windows XP Environment

If you are running the Virtual KVM Client or Active KVM Client in a Windows® XP environment, users must have Administrator privileges to access any virtual media type other than CD-ROM connections, ISOs and ISO images.

Virtual Media in a Linux Environment

Active System Partitions

You cannot mount active system partitions from a Linux client.

Linux Ext3/4 drive partitions need to be unmounted via `umount /dev/<device label>` prior to making a virtual media connection.

Mapped Drives

Mapped drives from Linux clients are not locked when mounted onto connected targets. This applies only to KX III 2.4.0 (and later).

Drive Partitions

The following drive partition limitations exist across operating systems:

- Windows® and Mac targets are not able to read Linux formatted partitions
- Windows and Linux cannot read Mac formatted partitions
- Only Windows Fat partitions are supported by Linux

Root User Permission Requirement

Your virtual media connection can be closed if you mount a CD ROM from a Linux client to a target and then unmount the CD ROM.

To avoid these issues, you must be a root user.

Connect Drive Permissions (Linux)

Users must have the appropriate access permissions in order to connect the Drive/CD-ROM to the target. This can be checked using:

```
guest_user@administrator-desktop:~$ ls -l /dev/sr0
brw-rw----+ 1 root cdrom 11, 12-03-2010 11:52 /dev/sr0
```

In the above example, the permission must be changed to allow read access.

On a system that supports ACLs in its file utilities, the `ls` command changes its behavior in the following way:

- For files that have a default ACL or an access ACL that contains more than the three required ACL entries, the `ls(1)` utility in the long form produced by `ls -l` displays a plus sign (+) after the permission string.

This is indicated in the example provided here for `/dev/sr0`, use `getfacl -a /dev/sr0` to see if the user has been provided access as part of an ACL. In this case they have and are therefore able to connect the cd-rom onto the target even though the output of the `ls -l` command may indicate otherwise.

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

A similar check of the permissions for a removable device shows:

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

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

This requires that the user is provided read-only permissions for the removable device:

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

The drive is then available to connect to the target.

Virtual Media in a Mac Environment

Active System Partition

You cannot use virtual media to mount active system partitions for a Mac client.

Drive Partitions

The following drive partition limitations exist across operating systems:

- Windows® and Mac targets are not able to read Linux formatted partitions
- Windows cannot read Mac formatted partitions
- Windows FAT and NTFS are supported by Mac
- Mac users must unmount any devices that are already mounted in order to connect to a target server. Use `>diskutil unmount /dev/disk1s1` to unmount the device and `diskutil mount /dev/disk1s1` to remount it.

Connect Drive Permissions (Mac)

In order for a device to be available to connect to a target from a Mac® client, you must have read-only permissions to the removable device:

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

Virtual Media File Server Setup (File Server ISO Images Only)

This feature is only required when using virtual media to access file server ISO images. ISO9660 format is the standard supported by Raritan. However, other CD-ROM extensions may also work.

Note: SMB/CIFS support is required on the file server.

Use the Remote Console File Server Setup page to designate the files server(s) and image paths that you want to access using virtual media. File server ISO images specified here are available for selection in the Remote Server ISO Image Hostname and Image drop-down lists in the Map Virtual Media CD/ISO Image dialog. See **Mounting CD-ROM/DVD-ROM/ISO Images** (on page 248).

► **To designate file server ISO images for virtual media access:**

1. Choose Virtual Media from the Remote Console. The File Server Setup page opens.
2. Check the Selected checkbox for all media that you want accessible as virtual media.
3. Enter information about the file server ISO images that you want to access:
 - IP Address/Host Name - Host name or IP address of the file server.
 - Image Path - Full path name of the location of the ISO image. For example, /sharename0/path0/image0.iso, \sharename1\path1\image1.iso, and so on.

Note: The host name cannot exceed 232 characters in length.

4. Click Save. All media specified here are now available for selection in the Map Virtual Media CD/ISO Image dialog.

Note: If you are connecting to a Windows 2003® server and attempt to load an ISO image from the server, you may receive an error stating "Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password".

If this occurs, disable "Microsoft Network Server: Digitally Sign Communications" option on the server under the Domain Controllers policies.

Chapter 5 KX III KVM Clients

KVM Client	Name	Platform	Features
Active KVM Client	AKC	Windows Platforms Requires Microsoft .NET	Full-featured KVM Client Java-Free
Virtual KVM Client	VKC	Linux & Mac Requires Java	Full-featured KVM Client Requires Java
HTML KVM Client	HKC	Linux & Mac Windows w/o .NET HTML & Javascript	Basic KVM Access Only Java-Free

- AKC is best for Windows Platforms
- VKC is best for Linux and Mac users with Java
- HKC is best for Linux and Mac users without Java

*Note: Many features are supported on HKC. See **HTML KVM Client (HKC) Help** (on page 305) for details.*

In This Chapter

KX III KVM Client Launching	255
Virtual KVM Client (VKC and VKCs) Help	256
Active KVM Client (AKC) Help	301
HTML KVM Client (HKC) Help	305

KX III KVM Client Launching

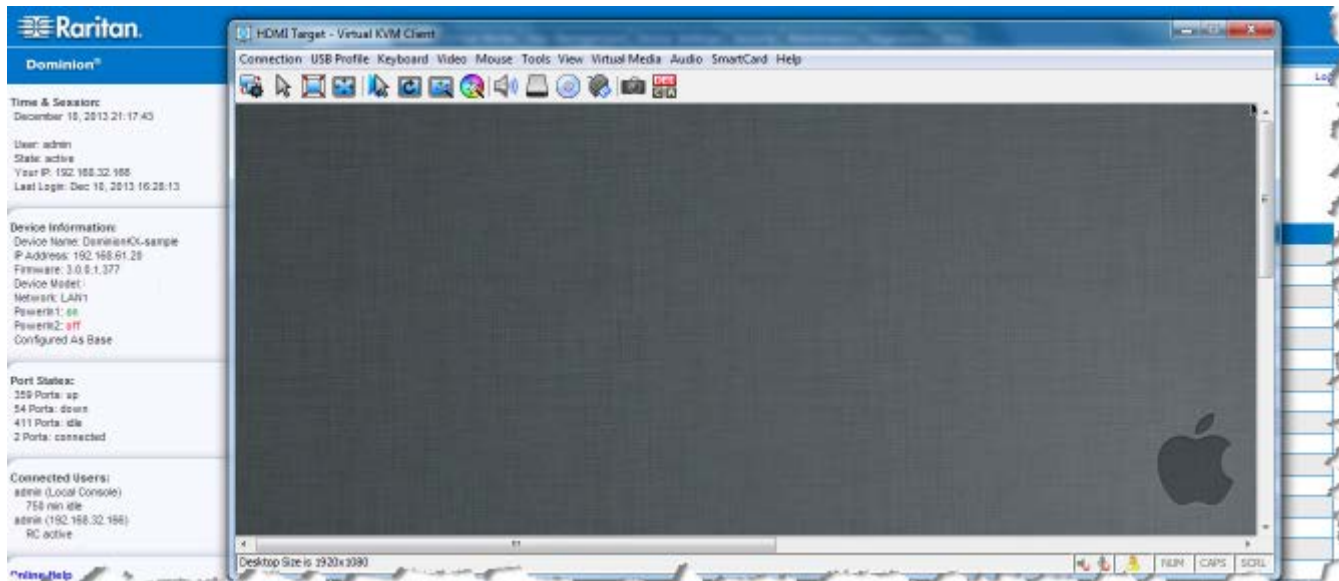
KVM Client	Name	Underlying Technology	Automatically Launched For	URL to Force Launch
Active KVM Client	AKC	Microsoft .NET Framework	Windows & .NET Framework	<KX3 IP Address>/ akc
Virtual KVM Client	VKC	Oracle Java	Non-Windows with Java	<KX3 IP Address>/ vk c
HTML KVM Client	HKC	Browser HTML & Javascript	Non-Windows without Java	<KX3 IP Address>/ h kc

Virtual KVM Client (VKC and VKCs) Help

Overview

VKC is the default client for Non-Windows platform clients with Java.

Whenever you access a target server from the Port Access page of KX III the Remote Console, a Virtual KVM Client (VKC) window opens.



There is one Virtual KVM Client for each target server connected.

Virtual KVM Client windows can be minimized, maximized, and moved around your computer desktop.

IMPORTANT: Refreshing your browser closes the Virtual KVM Client connection.

Recommended Minimum Virtual KVM Client (VKC) Requirements

Raritan recommends the Virtual KVM Client (VKC) machines meet the following minimum requirements for use with KX III.

- Client machine with either a -
 - 'modern' dual-core CPU for a single connections, or
 - 'modern' quad core CPU for two or more simultaneous connections
- 4GB of RAM
 - VKC requires 50MB of RAM per connection

Virtual KVM Client Java Requirements

Java™ 1.7 is required to use the Java-based Virtual KVM Client (VKC).

Java 1.8.0_40 is required to use the VKCS.

Java 7 is not supported, and a Java error displays if you attempt to launch VKCS with JRE 1.7.

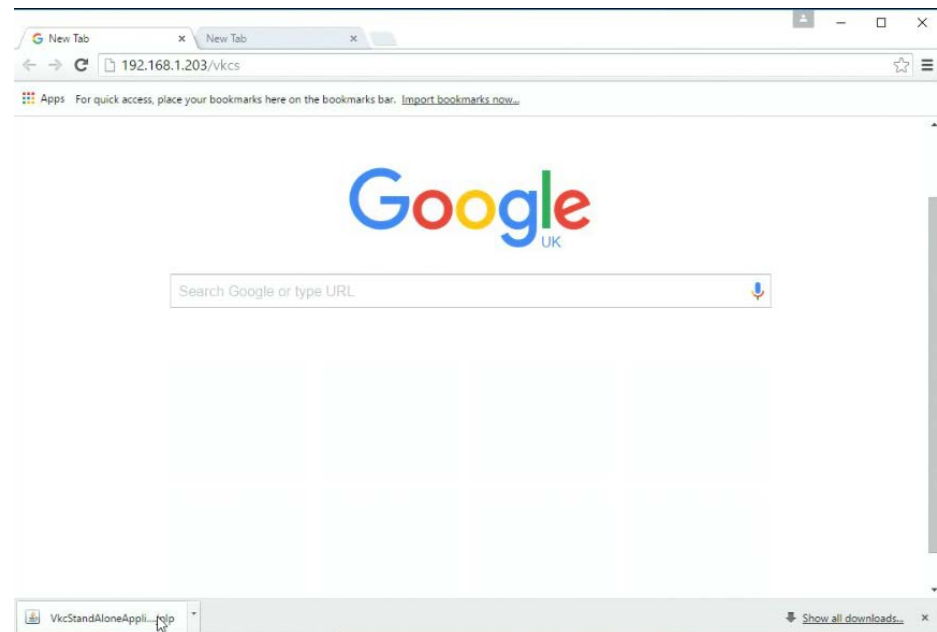
If Java is not installed, a prompt is displayed that the file cannot be opened, with an option to search for the program.

Note: VKC cannot be launched from Edge, Chrome 45 or later, Firefox 42 or later. VKCS is recommended for these browsers.

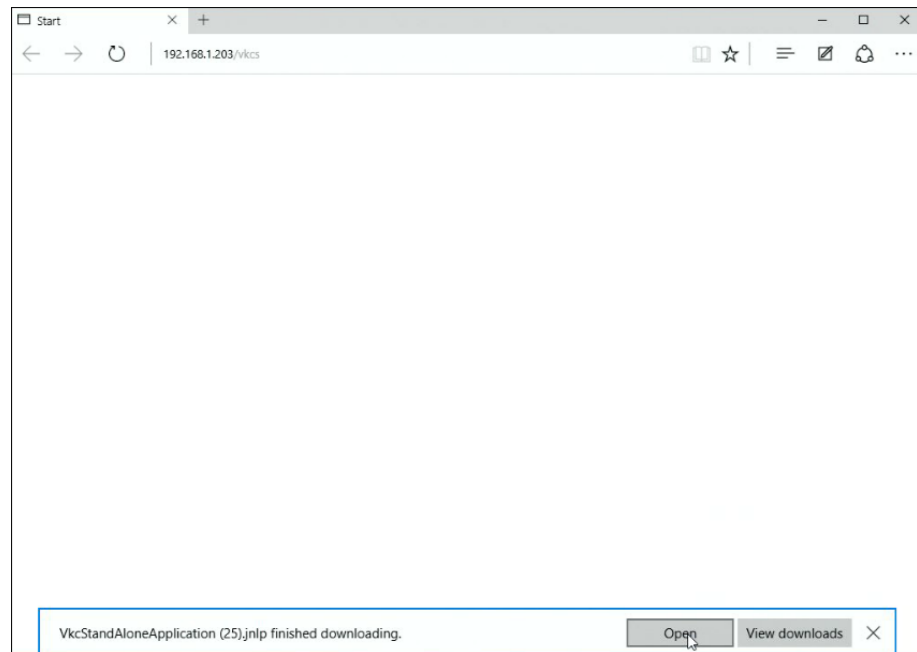
► VKCS Launching:

For all browsers, the VKCS standalone application needs to be downloaded everytime you use it.

- Chrome: The downloaded VKCS jnlp file must always be clicked at bottom left corner of browser window to launch.



- Edge: You must click Open at the bottom of the browser to launch.



- Internet Explorer: Launches automatically.
- Firefox: Use the option "Do this automatically for files like this from now on", when the vkcs.jnlp file downloads, and it will launch automatically in future

Proxy Server Configuration for Use with VKC, VKCS, and AKC

When the use of a Proxy Server is required, a SOCKS proxy must also be provided and configured on the remote client PC.

Note: If the installed proxy server is only capable of the HTTP proxy protocol, you cannot connect.

► **To configure the SOCKS proxy:**

1. On the remote client PC, select Control Panel > Internet Options.
 - a. On the Connections tab, click 'LAN settings'. The Local Area Network (LAN) Settings dialog opens.
 - b. Select 'Use a proxy server for your LAN'.
 - c. Click Advanced. The Proxy Settings dialog opens.
 - d. Configure the proxy servers for all protocols.

IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

- e. Click OK at each dialog to apply the settings.
2. Next, configure the proxy settings for the Java™ applets:
 - a. Select Control Panel > Java.
 - b. On the General tab, click Network Settings. The Network Settings dialog opens.
 - c. Select "Use Proxy Server".
 - d. Click Advanced. The Advanced Network Settings dialog opens.
 - e. Configure the proxy servers for all protocols.

IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

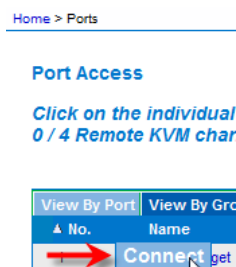
Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

Connect to a Target from Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC)

Once you have logged on to the KX III Remote Console, access target servers via the Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC).

► To connect to an available server:

1. On the Port Access page, click on the port name of the target server you want to connect to. The Port Action menu opens.
2. Click Connect.



See **Port Action Menu** (on page 24) for details on additional available menu options.

Configuring Connection Properties

Connection properties manage streaming video performance over remote connections to target servers.

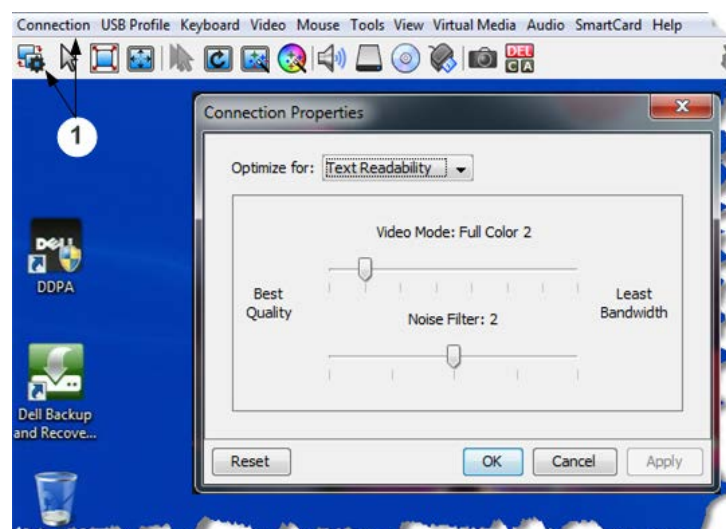
The properties are applied only to your connection - they do not impact the connection of other users accessing the same target servers.

If you make changes to connection properties, they are retained by the client.

Access Connection Properties

► To access connection properties:

- 1 Click Connection > Properties, or click the Connection... icon to open the Connection Properties dialog.



Default Connection Property Settings - Optimized for Best Performance

The KX III comes configured to provide optimal performance for the majority of video streaming conditions.

Default connection settings are:

- Optimized for: Text Readability - video modes are designed to maximize text readability.

This setting is ideal for general IT and computer applications, such as performing server administration.

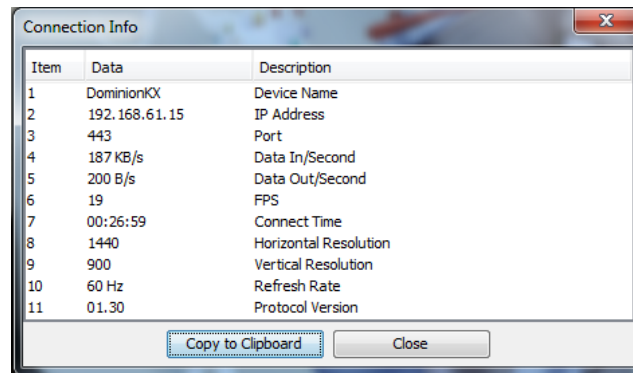
- Video Mode - defaults to Full Color 2.
Video frames transmit in high-quality, 24-bit color. This setting is suitable where a high-speed LAN is used.

- Noise Filter - defaults to 2.

The noise filter setting does not often need to be changed.

Click Reset on the Connection Properties dialog at any time to return to the default settings.

*Tip: Use the Connection Information dialog to monitor the connection in real-time. See **Access and Copy Connection Information** (on page 264)*



Item	Data	Description
1	DominionKX	Device Name
2	192.168.61.15	IP Address
3	443	Port
4	187 KB/s	Data In/Second
5	200 B/s	Data Out/Second
6	19	FPS
7	00:26:59	Connect Time
8	1440	Horizontal Resolution
9	900	Vertical Resolution
10	60 Hz	Refresh Rate
11	01.30	Protocol Version

Buttons: Copy to Clipboard, Close

Optimize for: Selections

Text Readability

Text Readability is designed to provide video modes with lower color depth but text remains readable. Greyscale modes are even available when applying lower bandwidth settings.

This setting is ideal when working with computer GUIs, such as server administration.

When working in full color video modes, a slight contrast boost is provided, and text is sharper.

In lower quality video modes, bandwidth is decreased at the expense of accuracy.

Color Accuracy

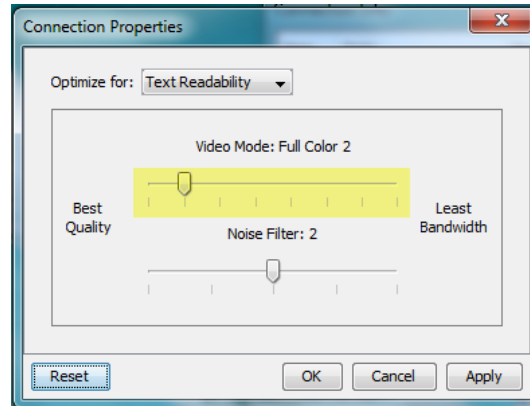
When Color Accuracy is selected, all video modes are rendered in full 24-bit color with more compression artifacts.

This setting applies to viewing video streams such as movies or other broadcast streams.

In lower quality video modes, sharpness of fine detail, such as text, is sacrificed.

Video Mode

The Video Mode slider controls each video frame's encoding, affecting video quality, frame rate and bandwidth.



In general, moving the slider to the left results in higher quality at the cost of higher bandwidth and, in some cases, lower frame rate.

Moving the slider to the right enables stronger compression, reducing the bandwidth per frame, but video quality is reduced.

In situations where system bandwidth is a limiting factor, moving the video mode slider to the right can result in higher frame rates.

When Text Readability is selected as the Optimized setting, the four rightmost modes provide reduced color resolution or no color at all.

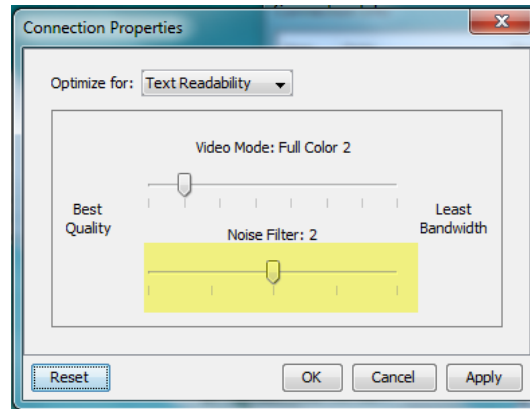
These modes are appropriate for administration work where text and GUI elements take priority, and bandwidth is at a premium.

Click Reset on the Connection Properties dialog at any time to return to the default settings.

Noise Filter

Unless there is a specific need to do so, do not change the noise filter setting. The default setting is designed to work well in most situations.

The Noise Filter controls how much interframe noise is absorbed by the KX III.



Moving the Noise Filter slider to the left lowers the filter threshold, resulting in higher dynamic video quality. However, more noise is likely to come through, resulting in higher bandwidth and lower frame rates.

Moving the slider to the right raises the threshold, allows less noise and less bandwidth is used. Video artifacts may be increased.

Moving the noise filter to the right may be useful when accessing a computer GUI over severely bandwidth-limited connections.

Click Reset on the Connection Properties dialog at any time to return to the default settings.

Connection Information

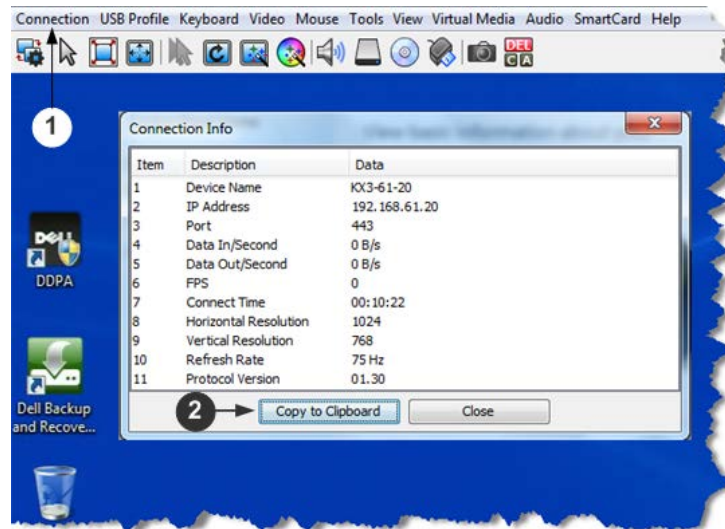
Open the Connection Information dialog for real-time connection information on your current connection, and copy the information from the dialog as needed.

See *Configuring Connection Properties* (on page 260)

► Current connection information:

- Name of the KX III
- IP address of the KX III
- Port - The KVM communication TCP/IP port used to access KX III.
- Data In/Second - Data rate received from the KX III
- Data Out/Second - Data rate sent to the KX III.
- Connect Time - The duration of the current connection.
- FPS - Video frames per second transmitted received from the KX III.
- Horizontal Resolution - The target server horizontal resolution.
- Vertical Resolution - The target server vertical resolution.
- Refresh Rate - Refresh rate of the target server.
- Protocol Version - Raritan communications protocol version.

Access and Copy Connection Information



Steps

1	Click Connection > Info... to open the Connection Info dialog.
2	Click Copy to Clipboard. Paste the information as needed.

USB Profiles

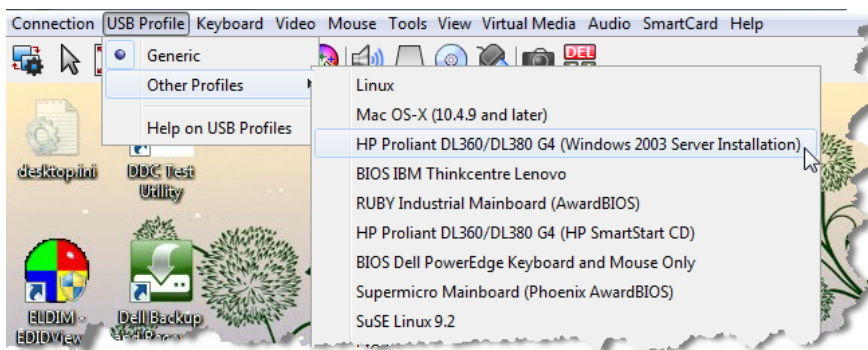
Select a USB profile that best applies to the KVM target server.

For example, if the server is running Windows® operating system, it would be best to use the Generic profile.

Or, to change settings in the BIOS menu or boot from a virtual media drive, depending on the target server model, a BIOS profile may be more appropriate.

► **To set a USB profile for a target server:**

- Choose USB Profile, then choose Generic, or choose Other Profiles to select from a menu.



► **To view details on USB profiles:**

- Choose USB Profile > Help on USB Profiles.

Keyboard

Send Ctrl+Alt+Del Macro

Due to its frequent use, a Ctrl+Alt+Delete macro is preprogrammed.

Selecting Keyboard > Send Ctrl+Alt+Del, or clicking on the

Ctrl+Alt+Delete button  in the toolbar sends this key sequence to the server or to the KVM switch to which you are currently connected.

In contrast, if you were to physically press the Ctrl+Alt+Del keys, the command would first be intercepted by your own PC due to the structure of the Windows operating system, instead of sending the key sequence to the target server as intended.

Send LeftAlt+Tab (Switch Between Open Windows on a Target Server)

Select Keyboard > Send LeftAlt + Tab to switch between open windows on the target server or KVM switch you are connected to.

Setting CIM Keyboard/Mouse Options

► To access the DCIM-USBG2 setup menu:

1. Put the mouse focus on a window such as Note Pad (Windows® operating system) or an equivalent.
2. Select Set CIM Keyboard/Mouse options. This is the equivalent of sending the Left-Control and Num Lock to the target. The CIM setup menu options are then displayed.
3. Set the language and mouse settings.
4. Exit the menu to return to normal CIM functionality.

Send Text to Target

► To use the Send Text to Target function for the macro:

1. Click the Keyboard > Send Text to Target. The Send Text to Target dialog appears.
2. Enter the text you want sent to the target.

Note: Non-English characters are not supported by the Send Text to Target function.

3. If the target uses a US/International keyboard layout, select the "Target system is set to the US/International keyboard layout" checkbox.
4. Click OK.

Keyboard Macros

Keyboard macros ensure that keystroke combinations intended for the target server are sent to and interpreted only by the target server. Otherwise, they might be interpreted by your client PC.

Macros are stored on the client PC and are PC-specific. If you use another PC, you cannot see your macros.

In addition, if another person uses your PC and logs in under a different name, that user will see your macros since they are computer-wide.

Build a New Macro

► To build a macro:

1. Click Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.
2. Click Add. The Add Keyboard Macro dialog appears.
3. Type a name for the macro in the Keyboard Macro Name field. This name appears in the Keyboard menu after it is created.
4. From the Hot-Key Combination field, select a keyboard combination from the drop-down list. This allows you to execute the macro with a predefined keystroke. **Optional**
5. In the Keys to Press drop-down list, select each key you would like to use to emulate the keystrokes that is used to perform the command. Select the keys in the order by which they are to be pressed. After each selection, select Add Key. As each key is selected, it appears in the Macro Sequence field and a Release Key command is automatically added after each selection.

For example, create a macro to close a window by selecting Left Ctrl + Esc. This appears in the Macro Sequence box as follows:

Press Left Alt

Press F4

Esc

Release F4

Esc

Release Left Alt

6. Review the Macro Sequence field to be sure the macro sequence is defined correctly.
 - a. To remove a step in the sequence, select it and click Remove.
 - b. To change the order of steps in the sequence, click the step and then click the up or down arrow buttons to reorder them as needed.

7. Click OK to save the macro. Click Clear to clear all field and start over. When you click OK, the Keyboard Macros dialog appears and lists the new keyboard macro.
8. Click Close to close the Keyboard Macros dialog. The macro now appears on the Keyboard menu in the application.
9. Select the new macro on the menu to run it or use the keystrokes you assigned to the macro.

Importing and Exporting Macros

Macros created in VKC cannot be used in AKC or vice versa. Macros created on HKC are only compatible with HKC, and cannot be used on AKC or VKC. Likewise, macros created on VKC or AKC cannot be used on HKC.

Import Macros

► To import macros:

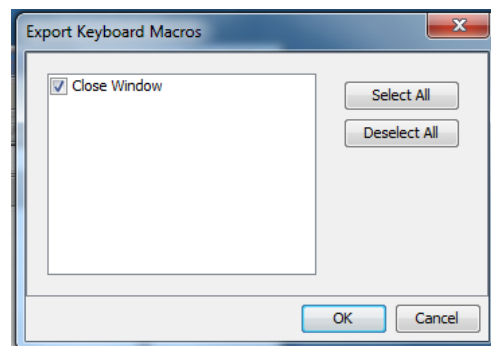
1. Choose Keyboard > Import Keyboard Macros to open the Import Macros dialog. Browse to the folder location of the macro file.
2. Click on the macro file and click Open to import the macro.
 - a. If too many macros are found in the file, an error message is displayed and the import terminates once OK is selected.
 - b. If the import fails, an error dialog appears and a message regarding why the import failed is displayed. Select OK to continue the import without importing the macros that cannot be imported.
3. Select the macros to be imported by checking their corresponding checkbox or using the Select All or Deselect All options.
4. Click OK to begin the import.
 - a. If a duplicate macro is found, the Import Macros dialog appears. Do one of the following:

- Click Yes to replace the existing macro with the imported version.
 - Click Yes to All to replace the currently selected and any other duplicate macros that are found.
 - Click No to keep the original macro and proceed to the next macro
 - Click No to All keep the original macro and proceed to the next macro. Any other duplicates that are found are skipped as well.
 - Click Cancel to stop the import.
 - Alternatively, click Rename to rename the macro and import it. If Rename is selected, the Rename Macro dialog appears. Enter a new name for the macro in the field and click OK. The dialog closes and the process proceeds. If the name that is entered is a duplicate of a macro, an alert appears and you are required to enter another name for the macro.
- b. If during the import process the number of allowed, imported macros is exceeded, a dialog appears. Click OK to attempt to continue importing macros or click Cancel to stop the import process.

The macros are then imported. If a macro is imported that contains a hot key that already exists, the hot key for the imported macro is discarded.

Export Macros

1. Choose Tools > Export Macros to open the Select Keyboard Macros to Export dialog.



2. Select the macros to be exported by checking their corresponding checkbox or using the Select All or Deselect All options.
3. Click Ok. An "Export Keyboard Macros to" dialog is displayed. Locate and select the macro file. By default, the macro exists on your desktop.

4. Select the folder to save the macro file to, enter a name for the file and click Save. If the macro already exists, you receive an alert message.
5. Select Yes to overwrite the existing macro or No to close the alert without overwriting the macro.

Video Properties

Refreshing the Screen

The Refresh Screen command forces a refresh of the video screen. Video settings can be refreshed automatically in several ways:

- The Refresh Screen command forces a refresh of the video screen.
- The Auto-sense Video Settings command automatically detects the target server's video settings.
- The Calibrate Color command calibrates the video to enhance the colors being displayed.

In addition, you can manually adjust the settings using the Video Settings command.

► **To refresh the video settings, do one of the following:**

- Choose Video > Refresh Screen, or click the Refresh Screen button  in the toolbar.

Auto-Sense Video Settings

The Auto-sense Video Settings command forces a re-sensing of the video settings (resolution, refresh rate) and redraws the video screen.

► **To automatically detect the video settings:**

- Choose Video > Auto-sense Video Settings, or click the Auto-Sense Video Settings button  in the toolbar.

A message stating that the auto adjustment is in progress appears.

Calibrating Color

Use the Calibrate Color command to optimize the color levels (hue, brightness, saturation) of the transmitted video images.

The color settings are on a target server-basis.

*Note: When color is successfully calibrated, the values are cached and reused each time you switch to the target. Changes to the brightness and contrast in Video Settings are not cached. Changing resolution resets the video to the cached values again. You can clear the cached values in Video > Clear Video Settings Cache. See **Clear Video Settings Cache** (on page 271).*

► To calibrate the color:

- Choose Video > Calibrate Color, or click the Calibrate Color button



in the toolbar.

The target device screen updates its color calibration.

Clear Video Settings Cache

You can clear the video settings cache to delete old settings that do not apply anymore, such as when a target server is replaced. When you clear the video settings cache, the server automatically does a video auto-sense and color calibration. The new values are cached and reused when the target is accessed again.

► To clear the video settings cache:

- Choose Video > Clear Video Settings Cache in the toolbar.

Adjusting Video Settings

Use the Video Settings command to manually adjust the video settings.

► To change the video settings:

- Choose Video > Video Settings to open the Video Settings dialog.
- Adjust the following settings as required. As you adjust the settings the effects are immediately visible:
 - PLL Settings

Clock - Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended. Under most circumstances, this setting should not be changed because the autodetect is usually quite accurate.

Phase - Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.

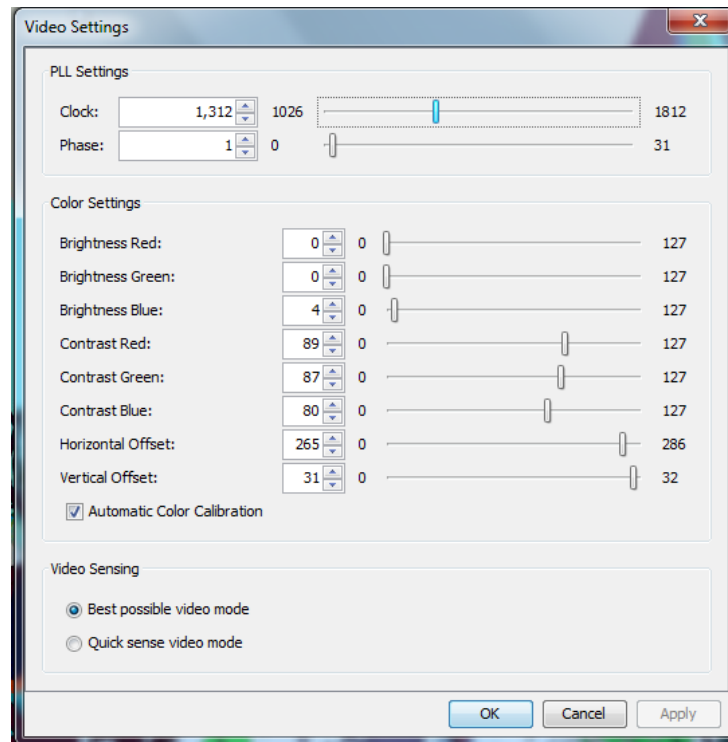
- b. Brightness: Use this setting to adjust the brightness of the target server display.
- c. Brightness Red - Controls the brightness of the target server display for the red signal.
- d. Brightness Green - Controls the brightness of the green signal.
- e. Brightness Blue - Controls the brightness of the blue signal.
- f. Contrast Red - Controls the red signal contrast.
- g. Contrast Green - Controls the green signal.
- h. Contrast Blue - Controls the blue signal.

If the video image looks extremely blurry or unfocused, the settings for clock and phase can be adjusted until a better image appears on the active target server.

Warning: Exercise caution when changing the Clock and Phase settings. Doing so may result in lost or distorted video and you may not be able to return to the previous state. Contact Raritan Technical Support before making any changes.

- i. Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor.
 - j. Vertical Offset - Controls the vertical positioning of the target server display on your monitor.
3. Select Automatic Color Calibration to enable this feature. This setting does not apply to KX3-808 target servers.
 4. Select the video sensing mode. This setting does not apply to KX3-808 target servers when connecting to the target, but will apply if you change resolution.
 - Best possible video mode
The device will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.
 - Quick sense video mode
With this option, the device will use a quick video Auto Sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.
 5. Click OK to apply the settings and close the dialog. Click Apply to apply the settings without closing the dialog.

Note: Some Sun background screens, such as screens with very dark borders, may not center precisely on certain Sun servers. Use a different background or place a lighter colored icon in the upper left corner of the screen.



Screenshot from Target Command (Target Screenshot)

Take a screenshot of a target server using the Screenshot from Target server command. If needed, save this screenshot to a file location of your choosing as a bitmap, JPEG or PNG file.

► To take a screenshot of the target server:

1. Select Video > Screenshot from Target, or click the Target Screenshot button  on the toolbar.
2. In the Save dialog, choose the location to save the file, name the file, and select a file format from the 'Files of type' drop-down.
3. Click Save to save the screenshot.

Mouse Options

You can operate in either single mouse mode or dual mouse mode.

When in a dual mouse mode, and provided the option is properly configured, the mouse cursors align.

When controlling a target server, the Remote Console displays two mouse cursors - one belonging to your KX III client workstation, and the other belonging to the target server.

When there are two mouse cursors, the device offers several mouse modes:

- Absolute (Mouse Synchronization)
- Intelligent (Mouse Mode)
- Standard (Mouse Mode)

When the mouse pointer lies within the KVM Client target server window, mouse movements and clicks are directly transmitted to the connected target server.

While in motion, the client mouse pointer slightly leads the target mouse pointer due to mouse acceleration settings.

On fast LAN connections, you can use single mouse mode, and view only the target server's pointer.

You can toggle between these two modes (single mouse and dual mouse).

Dual Mouse Modes

Absolute Mouse Synchronization

In this mode, absolute coordinates are used to keep the client and target cursors in synch, even when the target mouse is set to a different acceleration or speed.

This mode is supported on servers with USB ports and is the default mode for virtual media CIMs.

Absolute Mouse Synchronization requires the use of a virtual media CIM

-

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

► To enter Absolute Mouse Synchronization:

- Choose Mouse > Absolute from the KVM client.

The black USB connector on the DVUSB CIMs are used for the keyboard and mouse. The gray connector is used for virtual media.

Keep both USB plugs of the CIM connected to the device.

The device may not operate properly if both plugs are not connected to the target server.

Intelligent Mouse Mode

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target. Intelligent mouse mode is the default for non-VM targets.

Enter Intelligent Mouse Mode

► To enter intelligent mouse mode:

- Choose Mouse > Intelligent.

Intelligent Mouse Synchronization Conditions

The Intelligent Mouse Synchronization command, available on the Mouse menu, automatically synchronizes mouse cursors during moments of inactivity. For this to work properly, however, the following conditions must be met:

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- Advanced mouse properties such as “Enhanced pointer precision” or “Snap mouse to default button in dialogs” should be disabled.
- Choose “Best Possible Video Mode” in the Video Settings window.
- The edges of the target video should be clearly visible (that is, a black border should be visible between the target desktop and the remote KVM console window when you scroll to an edge of the target video image).
- When using the intelligent mouse synchronization function, having a file icon or folder icon located in the upper left corner of your desktop may cause the function not to work properly. To be sure to avoid any problems with this function, Raritan recommends you do not have file icons or folder icons in the upper left corner of your desktop.

After autosensing the target video, manually initiate mouse synchronization by clicking the Synchronize Mouse button on the toolbar. This also applies when the resolution of the target changes if the mouse cursors start to desync from each other.

If intelligent mouse synchronization fails, this mode will revert to standard mouse synchronization behavior.

Please note that mouse configurations will vary on different target operating systems. Consult your OS guidelines for further details. Also note that intelligent mouse synchronization does not work with UNIX targets.

Standard Mouse Mode

Standard Mouse mode uses a standard mouse synchronization algorithm. The algorithm determines relative mouse positions on the client and target server.

In order for the client and target mouse cursors to stay in synch, mouse acceleration must be disabled. Additionally, specific mouse parameters must be set correctly.

► **To enter Standard Mouse mode:**

- Choose Mouse > Standard.

Mouse Synchronization Tips

If you have an issue with mouse synchronization:

1. Verify that the selected video resolution and refresh rate are among those supported by the device. The KVM Client Connection Info dialog displays the actual values that the device is seeing.
2. Force an auto-sense by clicking the KVM Client auto-sense button.
3. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris KVM target servers):
 - a. Open a terminal window.
 - b. Enter the following command: `xset mouse 1 1`
 - c. Close the terminal window.
4. Click the "KVM Client mouse synchronization" button .

Synchronize Your Mouse

In dual mouse mode, the Synchronize Mouse command forces realignment of the target server mouse cursor with the client mouse cursor.

► **To synchronize the mouse cursors, do one of the following:**

- Click the Synchronize Mouse button  in the KVM client toolbar, or select Mouse > Synchronize Mouse from the menu bar.

Note: This option is available only in Standard and Intelligent mouse modes.

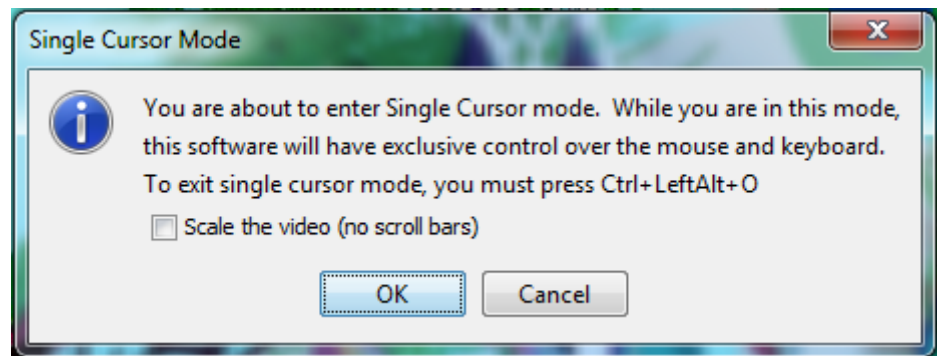
Single Mouse Mode

Single Mouse mode uses only the target server mouse cursor; the client mouse cursor no longer appears onscreen.

Note: Single mouse mode does not work on Windows or Linux targets when the client is running on a Virtual Machine.

► **To enter single mouse mode, do one the following:**

- Choose Mouse > Single Mouse Cursor.
- Click the Single/Double Mouse Cursor button  in the toolbar.



► **To exit single mouse mode:**

1. Press Ctrl+Alt+O on your keyboard to exit single mouse mode.

Tool Options

General Settings

► **To set the tools options:**

1. Click Tools > Options. The Options dialog appears.
2. Select the Enable Logging checkbox only if directed to by Technical Support.

This option creates a log file in your home directory.

3. Choose the Keyboard Type from the drop-down list (if necessary).

The options include:

- US/International
- French (France)
- German (Germany)
- Japanese
- United Kingdom

- Korean (Korea)
- French (Belgium)
- Norwegian (Norway)
- Portuguese (Portugal)
- Danish (Denmark)
- Swedish (Sweden)
- German (Switzerland)
- Hungarian (Hungary)
- Spanish (Spain)
- Italian (Italy)
- Slovenian
- Translation: French - US
- Translation: French - US International

In AKC, the keyboard type defaults to the local client, so this option does not apply.

4. Configure hotkeys:

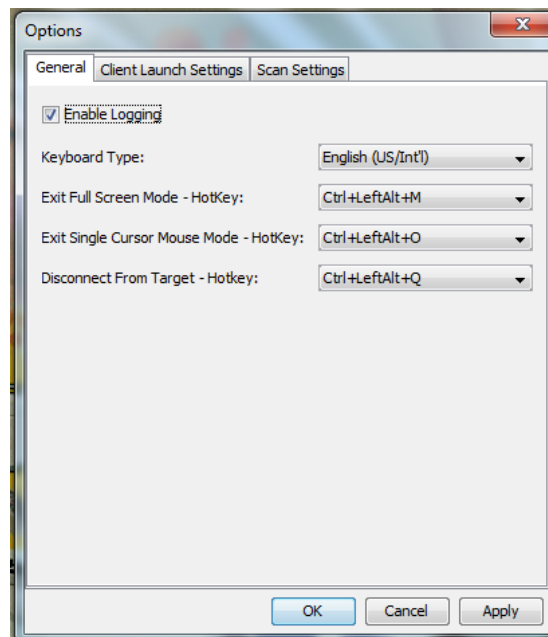
- Exit Full Screen Mode - Hotkey.
When you enter Full Screen mode, the display of the target server becomes full screen and acquires the same resolution as the target server.
This is the hot key used for exiting this mode.
- Exit Single Cursor Mode - Hotkey.
When you enter single cursor mode, only the target server mouse cursor is visible.
This is the hot key used to exit single cursor mode and bring back the client mouse cursor.
- Disconnect from Target - Hotkey.
Enable this hotkey to allow users to quickly disconnect from the target.

For hotkey combinations, the application does not allow you to assign the same hotkey combination to more than one function.

For example, if Q is already applied to the Disconnect from Target function, it won't be available for the Exit Full Screen Mode function.

Further, if a hotkey is added to the application due to an upgrade and the default value for the key is already in use, the next available value is applied to the function instead.

- Click OK.



Keyboard Limitations

Turkish Keyboards

If using a Turkish keyboard, you must connect to a target server through the Active KVM Client (AKC). It is not supported by other Raritan clients.

Slovenian Keyboards

The < key does not work on Slovenian keyboards due to a JRE limitation.

Language Configuration on Linux

Because the Sun JRE on Linux has problems generating the correct Key Events for foreign-language keyboards configured using System Preferences, Raritan recommends that you configure foreign keyboards using the methods described in the following table.

Language	Configuration method
US Intl	Default
French	Keyboard Indicator
German	System Settings (Control Center)
Japanese	System Settings (Control Center)
UK	System Settings (Control Center)
Korean	System Settings (Control Center)

Language	Configuration method
Belgian	Keyboard Indicator
Norwegian	Keyboard Indicator
Danish	Keyboard Indicator
Swedish	Keyboard Indicator
Hungarian	System Settings (Control Center)
Spanish	System Settings (Control Center)
Italian	System Settings (Control Center)
Slovenian	System Settings (Control Center)
Portuguese	System Settings (Control Center)

Note: The Keyboard Indicator should be used on Linux systems using Gnome as a desktop environment.

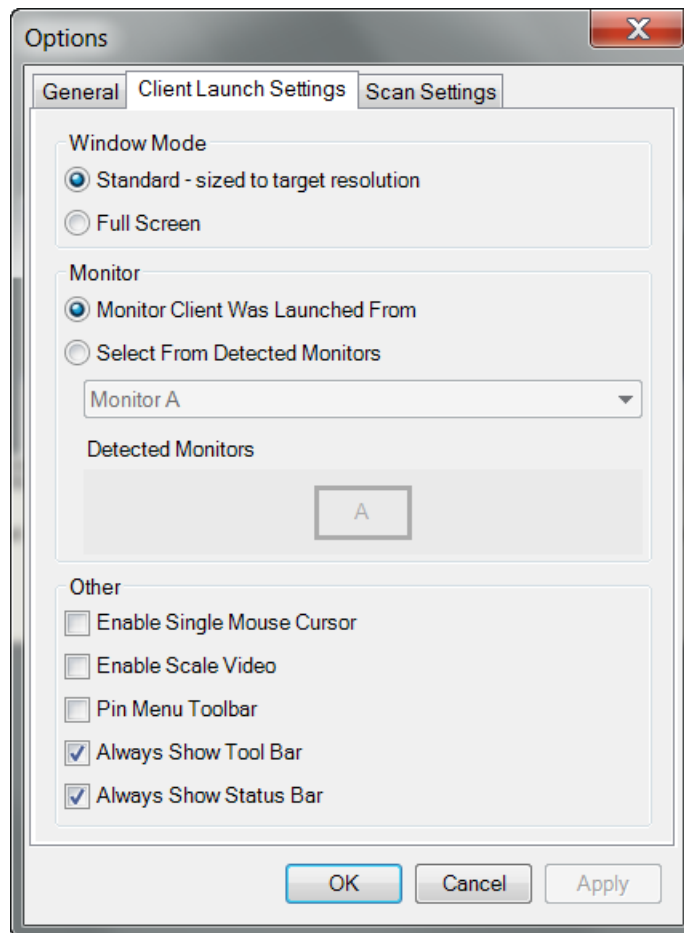
Client Launch Settings

Configuring client launch settings allows you to define the screen settings for a KVM session.

► To configure client launch settings:

1. Click Tools > Options. The Options dialog appears.
2. Click on the Client Launch Settings tab.
 - To configure the target window settings:
 - a. Select 'Standard - sized to target Resolution' to open the window using the target's current resolution. If the target resolution is greater than the client resolution, the target window covers as much screen area as possible and scroll bars are added (if needed).
 - b. Select 'Full Screen' to open the target window in full screen mode.
 - To configure the monitor on which the target viewer is launched:
 - a. Select 'Monitor Client Was Launched From' if you want the target viewer to be launched using the same display as the application that is being used on the client (for example, a web browser or applet).
 - b. Use 'Select From Detected Monitors' to select from a list of monitors that are currently detected by the application. If a previously selected monitor is no longer detected, 'Currently Selected Monitor Not Detected' is displayed.

- To configure additional launch settings:
 - a. Select 'Enable Single Cursor Mode' to enable single mouse mode as the default mouse mode when the server is accessed.
 - b. Select 'Enable Scale Video' to automatically scale the display on the target server when it is accessed.
 - c. Select 'Pin Menu Toolbar' if you want the toolbar to remain visible on the target when it is in Full Screen mode. By default, while the target is in Full Screen mode, the menu is only visible when you hover your mouse along the top of the screen.
 - d. Always Show Tool Bar and Always Show Status Bar are per-user settings that are stored in the computer you are accessing the client from, so if you use a different computer, the setting may be different. Select to keep tool bar and status bar visible as default, deselect to keep tool bar and status bar hidden as default.
- 3. Click OK.



Configuring Port Scan Settings in VKC/VKCS and AKC

Configuring port scan options in VKC/VKCS and AKC applies to scanning from the KX III Remote Console.

To configure port scan options for the Local Console, see ***Configure Local Console Scan Settings*** (on page 392)

Use the port scanning feature to search for selected targets, and display them in a slide show view, allowing you to monitor up to 32 targets at one time.

You can connect to targets or focus on a specific target as needed. Scans can include standard targets, blade servers, tiered Dominion devices, and KVM switch ports.

Configure scan settings from either the VKC/VKCS or AKC.

See ***Scanning Ports - Remote Console*** (on page 375)

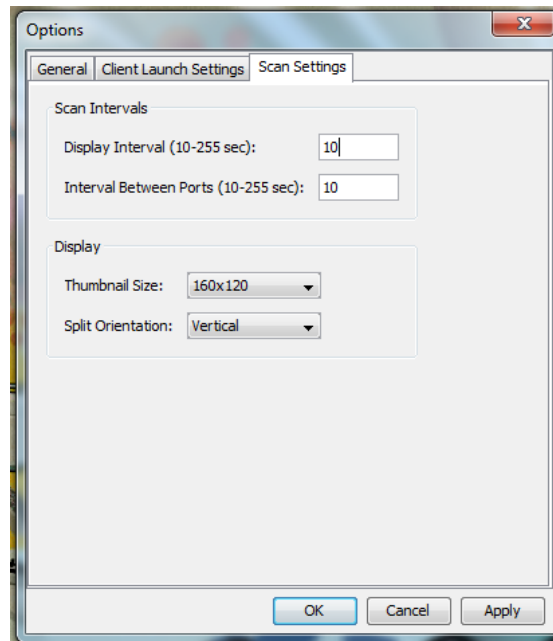
Use the Scan Settings tab to customize the scan interval and default display options.

Configure Port Scan

► To set scan settings:

1. Click Tools > Options. The Options dialog appears.
2. Select the Scan Settings tab.
3. In the "Display Interval (10-255 sec):" field, specify the number of seconds you want the target that is in focus to display in the center of the Port Scan window.
4. In the "Interval Between Ports (10 - 255 sec):" field, specify the interval at which the device should pause between ports.
5. In the Display section, change the default display options for the thumbnail size and split orientation of the Port Scan window.

6. Click OK.



Collecting a Diagnostic Snapshot of the Target

Administrators are able to collect a "snapshot" of a target from either the VKC/VKCS or Active KVM Client (AKC).

The "snapshot" function generate log files and image files from the target.

It then bundles these files in a zip file that can be sent to Raritan Technical Support in order to help diagnose technical problems you may be encountering.

The following files are included in the zip file:

- screenshot_image.png
This is a screenshot of the target that captures a picture of the issue you are experiencing. This feature is operates in the same as the "Screenshot from Target" feature.
- raw_video_image.png:
A snapshot image created from raw video data. Please note that client's postprocessing is applied, just as if it were a "regular" screen update.
- raw_video_ycbcr420.bin:
Binary file of the raw snapshot.
- raw_video_ycbcr420.txt:
Text file containing data used by Raritan to help diagnose issues.

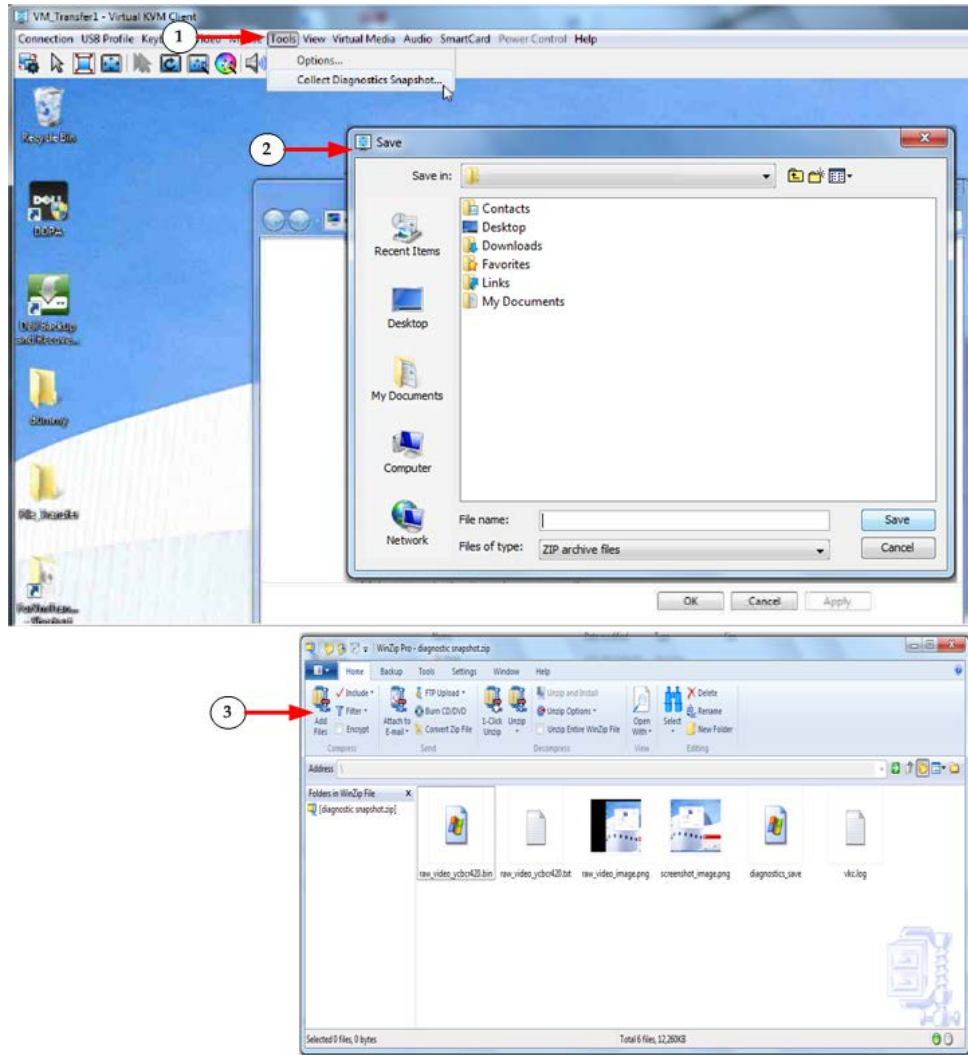
- Log.txt file:

These are the client logs.

Note that the logs are included even if you have not enabled information to be captured in them. VKC uses internal memory to capture the information in this case.

Collect a Diagnostic Snapshot from VKC, VKCS, and AKC

► To capture a diagnostic snapshot:



Steps

①	Access a target, and then click Tools > Collect a Diagnostic Snapshot. Several messages are displayed as the information is collected.
②	You are prompted to save the zip file containing the diagnostic files.
③	The zip file containing the diagnostic files that were collecting opens.

View Options

View Toolbar

You can use the Virtual KVM client with or without the toolbar display.

► **To toggle the display of the toolbar (on and off):**

- Choose View > View Toolbar.

View Status Bar

By default, the status bar is displayed at the bottom of the target window.

► **To hide the status bar:**

- Click View > Status Bar to deselect it.

► **To restore the status bar:**

- Click View > Status Bar to select it.

Scaling

Scaling your target window allows you to view the entire contents of the target server window.

This feature increases or reduces the size of the target video to fit the Virtual KVM Client window size, and maintains the aspect ratio so that you see the entire target server desktop without using the scroll bar.

► **To toggle scaling (on and off):**

- Choose View > Scaling.

Full Screen Mode

When you enter Full Screen mode, the target's full screen is displayed and acquires the same resolution as the target server.

The hot key used for exiting this mode is specified in the Options dialog, see *Tool Options* (on page 278).

While in Full Screen mode, moving your mouse to the top of the screen displays the Full Screen mode menu bar.

If you want the menu bar to remain visible while in Full Screen mode, enable the Pin Menu Toolbar option from the Tool Options dialog. See *Tool Options* (on page 278).

► To enter full screen mode:

- Choose View > Full Screen, or click the Full Screen button .

► To exit full screen mode:

- Press the hot key configured in the Tool's Options dialog. The default is Ctrl+Alt+M.

If you want to access the target in full screen mode at all times, you can make Full Screen mode the default.

► To set Full Screen mode as the default mode:

1. Click Tools > Options to open the Options dialog.
2. Select Enable Launch in Full Screen Mode and click OK.

Connect to Virtual Media

See *Virtual Media* (on page 243)

Smart Cards

Using the KX III, you are able to mount a smart card reader onto a target server to support smart card authentication and related applications.

For a list of supported smart cards, smart card readers, and additional system requirements, see ***Smart Card Minimum System Requirements, CIMs and Supported/Unsupported Smart Card Readers*** (on page 289).

Note: The USB Smart Card token (eToken NG-OTP) is only supported from the remote client.

Smart card reader mounting is also supported from the Local Console. See ***Local Console Smart Card Access*** (on page 394) in your Dominion device help.

Smart Card Minimum System Requirements, CIMs and Supported/Unsupported Smart Card Readers

Before you begin using a smart card reader, review the following:

- ***Smart Card Minimum System Requirements*** (on page 429)
- ***Supported Computer Interface Module (CIMs) Specifications*** (on page 421)
- Supported and Unsupported Smart Card Readers

Authentication When Accessing a Smart Card Reader

When accessing a server remotely, you can select an attached smart card reader and mount it onto the server.

Smart card authentication is used with the target server, it is not used to log into the device. Therefore, changes to smart card PIN and credentials do not require updates to device accounts.

PC Share Mode and Privacy Settings when Using Smart Cards

When PC-Share mode is enabled on the device, multiple users can share access to a target server.

However, when a smart card reader is connected to a target, the device will enforce privacy regardless of the PC-Share mode setting.

In addition, if you join a shared session on a target server, the smart card reader mounting will be disabled until exclusive access to the target server becomes available.

Smart Card Reader Detected

After a KVM session is established with a target server, a Smart Card menu and button are available in VKC and AKC.

Once the Smart Card button is selected or Smart Card is selected from the menu, the smart card readers that are detected as attached to the remote client are displayed in a dialog.

From this dialog, you can attach additional smart card readers, refresh the list of smart card readers attached to the target, and detach smart card readers.

You are also able to remove or reinsert a smart card. This function can be used to provide notification to a target server OS that requires a removal/reinsertion in order to display the appropriate login dialog. Using this function allows the notification to be sent to a single target without affecting other active KVM sessions.

Mount a Smart Card Reader

When mounted onto the target server, the card reader and smart card will cause the server to behave as if they had been directly attached.

Removal of the smart card or smart card reader will cause the user session to be locked or you will be logged out depending on how the card removal policy has been setup on the target server OS.

When the KVM session is terminated, either because it has been closed or because you switch to a new target, the smart card reader will be automatically unmounted from the target server.

► To mount a smart card reader from VKC or AKC:

1. Click the Smart Card menu and then select Smart Card Reader.

Alternatively, click the Smart Card button  in the toolbar.

2. Select the smart card reader from the Select Smart Card Reader dialog.
3. Click Mount.
4. A progress dialog will open. Check the 'Mount selected card reader automatically on connection to targets' checkbox to mount the smart card reader automatically the next time you connect to a target. Click OK to begin the mounting process.

Update a Smart Card Reader

- ▶ **To update the smart card in the Select Smart Card Reader dialog:**
 - Click Refresh List if a new smart card reader has been attached to the client PC.

Send Smart Card Remove and Reinsert Notifications

- ▶ **To send smart card remove and reinsert notifications to the target:**
 - Select the smart card reader that is currently mounted and click the Remove/Reinsert button.

Unmount (Remove) a Smart Card Reader

- ▶ **To unmount a smart card reader:**
 - Select the smart card reader to be unmounted and click the Unmount button.

Digital Audio

The KX III supports end-to-end, bidirectional, digital audio connections for digital audio playback and capture devices from a remote client to a target server.

The audio devices are accessed over a USB connection.

- Current device firmware is required.
- One of the following CIMs must be used:
 - D2CIM-DVUSB
 - D2CIM-DVUSB-DVI
 - D2CIM-DVUSB-HDMI

- D2CIM-DVUSB-DP

Windows®, Linux® and Mac® operating systems are supported. VKC, VKCS, and AKC support connections to audio devices.

Note: Audio CDs are not supported by virtual media so they do not work with the audio feature.

Before you begin using the audio feature, Raritan recommends you review the audio related information documented in the following sections of Help:

- ***Supported Audio Device Formats*** (on page 292)
- ***Recommendations for Dual Port Video*** (on page 234)
- ***Dual Video Port Group Supported Mouse Modes*** (on page 234)
- ***CIMs Required for Dual Video Support*** (on page 235)
- Informational Notes, ***Audio*** (on page 460)

Supported Audio Device Formats

The KX III supports one playback and capture device and one record device on a target at a time. The following audio device formats are supported:

- Stereo, 16 bit, 44.1K
- Mono, 16 bit, 44.1K
- Stereo, 16 bit, 22.05K
- Mono, 16 bit, 22.05K
- Stereo, 16 bit, 11.025K
- Mono, 16 bit, 11.025K

Digital Audio VKC and AKC Icons

Audio icons	Icon name	Description
  	Speaker	These icons are located in status bar at the bottom of the client window. Green, blinking waves indicate an audio playback session is currently streaming. A black speaker icon is displayed when the session is muted. The icon is grayed out when no audio is connected.
  	Microphone	These icons are located in the status bar at the bottom of the client window. Red, blinking waves indicate an audio capture session is currently underway. The Speaker icon, indicating a playback session is streaming, is also displayed when a session is underway. A black Microphone icon is displayed when the session is muted. When the Microphone icon is grayed out, no audio is connected.

Audio Playback and Capture Recommendations and Requirements

Audio Level

- Set the target audio level to a mid-range setting.
For example, on a Windows® client, set the audio to 50 or lower.
- This setting must be configured through the playback or capture audio device, not from the client audio device control.

Recommendations for Audio Connections when PC Share Mode is Enabled

If you are using the audio feature while running PC Share mode, audio playback and capture are interrupted if an additional audio device is connected to the target.

For example, User A connects a playback device to Target1 and runs an audio playback application then User B connects a capture device to the same target. User A's playback session is interrupted and the audio application may need to be restarted.

The interruption occurs because the USB device needs to be re-enumerated with the new device configuration.

It may take some time for the target to install a driver for the new device. Audio applications may stop playback completely, go to the next track, or just continue playing.

The exact behavior is dependent on how the audio application is designed to handle a disconnect/reconnect event.

Bandwidth Requirements

The table below details the audio playback and capture bandwidth requirements to transport audio under each of the selected formats.

Audio format	Network bandwidth requirement
44.1 KHz, 16bit stereo	176 KB/s
44.1 KHz, 16bit mono	88.2 KB/s
2.05 KHz, 16bit stereo	88.2 KB/s
22.05 KHz, 16bit mono	44.1 KB/s
11.025 KHz, 16bit stereo	44.1 KB/s
11.025 KHz, 16bit mono	Audio 22.05 KB/s

In practice, the bandwidth used when an audio device connects to a target is higher due to the keyboard and video data consumed when opening and using an audio application on the target.

A general recommendation is to have at least a 1.5MB connection before running playback and capture.

However, high video-content, full-color connections using high-target screen resolutions consume much more bandwidth and impact the quality of the audio considerably.

To help mitigate quality degeneration, there are a number of recommended client settings that reduce the impact of video on audio quality at lower bandwidths:

- Connect audio playback at the lower quality formats. The impact of video consuming bandwidth is much less notable at 11k connections than at 44k
- Set the connection speed under Connection Properties to a value that best matches the client to server connection
- Under Connection Properties, set the color depth to as low a value as possible. Reducing the color depth to 8 bit color considerably reduces the bandwidth consumed
- Set Smoothing, to High. This will improve the appearance of the target video by reducing displayed video noise
- Under Video settings, set the Noise Filter to its highest setting of 7 (highest value) so less bandwidth is used for target screen changes

Saving Audio Settings

Audio device settings are applied on a per KX III device basis.

Once the audio devices settings are configured and saved on the KX III, the same settings are applied to it.

For example, you can configure a Windows® audio device to use a stereo, 16 bit, 44.1K format.

When you connect to different targets and use that Windows audio device, the stereo, 16 bit, 44.1K format is applied to each target server.

For both playback and recording devices, the device type, device format, and the buffer settings applied to the device are saved.

See ***Connecting and Disconnecting from a Digital Audio Device*** (on page 297) for information on connecting to and configuring an audio device, and ***Adjusting Capture and Playback Buffer Size (Audio Settings)*** for information on audio device buffer settings.

If you are using the audio feature while running PC Share mode and VM Share mode so multiple users can access the same audio device on a target at once, the audio device settings of the user who initiates the session are applied to all users who join the session.

So, when a user joins an audio session, the target machine settings are used. See ***Connecting to Multiple Targets from a Single Remote Client*** (on page 296).

Connecting to Multiple Targets from a Single Remote Client

Connect to audio on up to four (4) target servers at the same time from a single, remote client.

See ***Connecting and Disconnecting from a Digital Audio Device*** (on page 297) for information on connecting to audio devices.

A Speaker icon  is displayed in the status bar at the bottom of the client window. It is grayed out when no audio is being used. When the

Speaker icon and Microphone icon  are displayed in the status bar, the session is being captured as it is streamed.

Note: When an audio session is underway, be sure to keep the session active or change the KX III's idle timeout time so the audio session does not time out.

Operating System Audio Playback Support

Review the table shown here to see which Raritan client works with audio playback/capture for each operating system:

Operating system	Audio playback and capture supported by:
Windows®	• Active KVM Client (AKC) • Virtual KVM Client (VKC)
Linux®	• Virtual KVM Client (VKC)
Mac®	• Virtual KVM Client (VKC)

Connecting and Disconnecting from a Digital Audio Device

Audio device settings are applied on a per KX III device basis.

Once the audio devices settings are configured and saved on the KX III, the same settings are applied to it.

See ***Saving Audio Settings*** (on page 296) for more information.

*Note: If you are using the audio feature while running PC Share mode and VM Share mode, see **Audio Playback and Capture Recommendations and Requirements** (on page 293) for important information. See also **Connecting to Multiple Targets from a Single Remote Client** (on page 296).*

Connect to a Digital Audio Device

► To connect to an audio device:

1. Connect the audio device to the remote client PC prior to launching the browser connection to the KX III.
2. Connect to the target from the Port Access page.
3. Once connected, click the Audio button  in the toolbar.
The Connect Audio Device dialog appears. A list of available audio devices connected to the remote client PC is displayed.

Note: If there are no available audio devices connected to the remote client PC, the Audio icon is grayed out. .

4. Check Connect Playback Device if you are connecting to a playback device.
5. Select the device that you wish to connect from the drop-down list.

6. Select the audio format for the playback device from the Format: drop-down.

Note: Select the format that you wish to use based on the available network bandwidth. Formats with lower sampling rates consume less bandwidth and may tolerate more network congestion.

7. Select the "Mount selected playback device automatically on connection to target" checkbox to automatically connect an audio playback device when you connect to an audio supporting target.
8. Check Connect Recording Device if you are connecting a recording device.

Note: The device names listed in the Connect Recording Device drop-down are truncated to a maximum of 30 characters for Java clients.

9. Select the device that you wish to connect from the drop-down list.
10. Select the audio format for the recording device from the Format: drop-down.
11. Click OK. If the audio connection is established, a confirmation message appears. Click OK.

If the connection was not established, an error message appears.

Once an audio connection is established, the Audio menu changes to Disconnect Audio. The settings for the audio device are saved and applied to subsequent connections to the audio device.

A Speaker icon  is displayed in the status bar at the bottom of the client window. It is grayed out when no audio is being used. When the Speaker icon and Microphone icon  are displayed in the status bar, the session is being captured as it is streamed.

Disconnect from an Audio Device

► To disconnect from the audio device:

- Click the Audio icon  in the toolbar and select OK when you are prompted to confirm the disconnect. A confirmation message appears. Click OK.

Adjusting Capture and Playback Buffer Size (Audio Settings)

Once an audio device is connected, the capture and playback buffer size can be adjusted as needed.

This feature is useful for controlling the quality of the audio, which may be impacted by bandwidth limitations or network spikes.

Increasing the buffer size improves the audio quality but may impact the delivery speed.

The maximum available buffer size is 400 milliseconds since anything higher than that greatly impacts audio quality.

The buffer size can be adjusted whenever needed, including during an audio session.

Audio settings are configured in VKC or AKC.

Adjust Audio Settings**► To adjust audio settings:**

1. Select Audio Settings from the Audio menu. The Audio Settings dialog opens.
2. Adjust the capture and/or playback buffer size as needed. Click OK.



Power Control Using VKC, VKCS, and AKC

You can power on, power off, and power cycle a target through the outlet it is connected to.

Access the target, and then select a power control option from the Power Control menu.



The menu option is disabled if you do not have permission for power control, and when outlets are not associated with the port.

Version Information - Virtual KVM Client

This menu command provides version information about the Virtual KVM Client, in case you require assistance from Raritan Technical Support.

► **To obtain version information:**

1. Choose Help > About Raritan Virtual KVM Client.
2. Use the Copy to Clipboard button to copy the information contained in the dialog to a clipboard file so it can be accessed later when dealing with support (if needed).

Active KVM Client (AKC) Help

Overview

The Active KVM Client (AKC) is based on Microsoft Windows .NET® technology.

This allows you to run the client in a Windows environments without using the Java® Runtime Environment (JRE), which is required to run Raritan's Virtual KVM Client (VKC).

AKC is the default KX III client on Windows platforms with .NET Framework, and it also works with CC-SG.

AKC provides the same features as VKC with the exception of the following:

- Keyboard macros created in AKC cannot be used in any other client.
- Direct port access configuration (see *Enabling Direct Port Access via URL* (on page 149))
- AKC server certification validation configuration (see *Prerequisites for Using AKC* (on page 302))
- AKC automatically loads favorites, VKC does not. See *Managing Favorites* (on page 381)

For details on using the features, see *Virtual KVM Client (VKC) Help* (see "*Virtual KVM Client (VKC and VKCs) Help*" on page 256).

Recommended Minimum Active KVM Client (AKC) Requirements

Raritan recommends the Active KVM Client (AKC) machines meet the following minimum requirements for use with KX III.

- Client machine with either a -
 - 'modern' dual-core CPU for a single connections, or
 - 'modern' quad core CPU for two or more simultaneous connections
- 4GB of RAM

AKC Supported Microsoft .NET Framework

The Active KVM Client (AKC) requires Windows .NET® version 4.0 or 4.5.

AKC Supported Operating Systems

When launched from Internet Explorer®, the Active KVM Client (AKC) allows you to reach target servers via the KX III.

AKC is compatible with the following platforms:

- Windows XP® operating system
- Windows Vista® operating system (up to 64 bit)
- Windows 7® operating system (up to 64 bit)
- Windows 8® operating system (up to 64 bit)
- Windows 10 ® operating system (up to 64 bit)

Note: You must be using Windows 7 if WINDOWS PC FIPs is turned on and you are accessing a target using AKC and a smartcard.

Since .NET is required to run AKC, if you do not have .NET installed or you have an unsupported version of .NET installed, you will receive a message instructing you to check the .NET version.

Note: Raritan recommends Windows XP® operating system users verify you have a working version of .NET 4.0 or 4.5 already installed before you launch AKC. If you do not verify your .NET version is working, you may be prompted to download a file versus receiving the default message to check your .NET version.

AKC Supported Browsers

- Internet Explorer® 10 (and later)
- Chrome on Windows platforms. You must have the Chrome ClickOnce plugin installed.

Prerequisites for Using AKC

Allow Cookies

Ensure the cookies from the IP address of the device that is being accessed are not currently being blocked.

Include KX III IP Address in 'Trusted Sites Zone'

Windows Vista®, Windows® 7 and Windows 2008 server users should ensure that the IP address of the device being accessed is included in their browser's Trusted Sites Zone.

Disable 'Protected Mode'

Windows Vista®, Windows® 7 and Windows 2008 server users should ensure that Protected Mode is not on when accessing the Raritan device.

Enable AKC Download Server Certificate Validation

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

- Administrators must upload a valid certificate to the device or generate a self-signed certificate on the device. The certificate must have a valid host designation.
- Each user must add the CA certificate (or a copy of self-signed certificate) to the Trusted Root CA store in their browser.

Proxy Server Configuration for Use with VKC, VKCS, and AKC

When the use of a Proxy Server is required, a SOCKS proxy must also be provided and configured on the remote client PC.

Note: If the installed proxy server is only capable of the HTTP proxy protocol, you cannot connect.

► **To configure the SOCKS proxy:**

1. On the remote client PC, select Control Panel > Internet Options.
 - a. On the Connections tab, click 'LAN settings'. The Local Area Network (LAN) Settings dialog opens.
 - b. Select 'Use a proxy server for your LAN'.
 - c. Click Advanced. The Proxy Settings dialog opens.
 - d. Configure the proxy servers for all protocols.

IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

- e. Click OK at each dialog to apply the settings.
2. Next, configure the proxy settings for the Java™ applets:
 - a. Select Control Panel > Java.
 - b. On the General tab, click Network Settings. The Network Settings dialog opens.
 - c. Select "Use Proxy Server".
 - d. Click Advanced. The Advanced Network Settings dialog opens.
 - e. Configure the proxy servers for all protocols.

IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

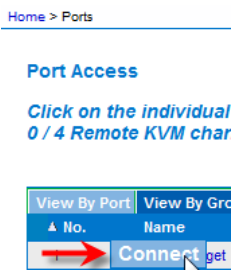
Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

Connect to a Target from Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC)

Once you have logged on to the KX III Remote Console, access target servers via the Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC).

► **To connect to an available server:**

- 1. On the Port Access page, click on the port name of the target server you want to connect to. The Port Action menu opens.
- 2. Click Connect.



See **Port Action Menu** (on page 24) for details on additional available menu options.

HTML KVM Client (HKC) Help

The HTML KVM client (HKC) provides KVM over IP access that runs in the browser without applets or browser plugins. HKC uses Javascript, NOT Java.

HKC runs on Linux and Mac clients, and on Windows clients without .NET in Internet Explorer 11 (not supported in IE 10 or lower), Edge, Firefox, Chrome and Safari browsers. See ***KX III KVM Client Launching*** (on page 255) for a full matrix of clients.

Many KVM features are supported. Future releases will provide more advanced KVM features.

► Supported Features:

- Connection Properties
- USB Profiles
- Video Settings
- Input Settings
- Audio Playback
- Virtual Media
- Power Control
- Dual Video Targets on IE, Edge, Firefox and Chrome
- Keyboard Macros
- Import and Export of Keyboard Macros
- Send Text to Target
- Keyboard and Mouse Settings
- Single Mouse Mode - available on Edge or Safari browsers

► Not supported:

- Smartcard
- Tools Menu for setting Client launch settings
- Port Scanning
- Limited keyboard support: US-English, UK-English, French, and German are supported
- Hotkeys for keyboard macros
- Pre-populated keyboard macros for Sun targets
- Can only create Macros from keys that exist on the client PC (US-English, UK-English, French, or German), no special function keys
- Single Mouse mode - not available on IE
- Virtual Media r/w not supported
- Local file transfer supported by Chrome and Firefox browsers only

- USB drive connects
- Favorites
- Audio capture
- Dual video targets not supported on Safari. Use Chrome or Firefox to connect to dual video targets on Mac OS.

► **Known Issues:**

- When Single Mouse Mode in the Edge browser is selected for the first time, the user is prompted to turn off the local mouse pointer. Select the bottom part of the Yes button.
- Target connections from Chrome 61 running on Fedora requires HardWare Acceleration to be enabled.
- If erratic mouse response is seen in Single Mouse mode on Fedora clients using the default Gnome desktop, use the Gnome classic desktop.
- To enable scrollbars on Mac Browser target connections: On the OS menu bar, choose System Preferences > General > Show scroll bars: Always.
- Internet Explorer and Edge support only 6 sessions at a time. The error displayed when attempting to connect to a seventh target is "Error could not connect to target." For IE11, you can increase the sessions allowed in the Group policy editor. See <https://jwebsocket.org/documentation/reference-guide/internet-explorer-tips>.
- For IE11 and Edge IPv6 device connections, either use device hostname or literal IPv6 as UNC. See https://en.wikipedia.org/wiki/IPv6_address#Literal_IPv6_addresses_in_UNC_path_names
- For Mac/Safari IPv6 device connections, use device hostname.
- Client Keyboard input selection should be set for each device individually.
- If encountering issues on browsers that have previously connected to a version of KX3.3 that supported the HTML KVM client, it may be necessary to clear the Cache Web Content from the browser.
- To launch HKC automatically in Safari browser: Use `http://<IP Address>/hkc`, OR use `http://<IP Address>/` if "Java content on browser" is disabled in Java Control Panel, and "Java Plugin" is disabled in the browser.
- From Chrome running on Linux, to get ´ ` or ^, the key needs to be hit three times, or twice followed by a space.

- For Mac Client browsers, ensure that the device certificate is installed and trusted. The certificate Common name should match the IP address/Hostname used to connect to the device. See ***SSL Certificates*** (see "***SSL and TLS Certificates***" on page 200) for information on creating and installing certificates
- On a default build of Redhat 7/Firefox ESR 24.5, there is no target video displayed on HKC connections. Older versions of Firefox lack HTML5 functions needed to support HKC. Upgrade Firefox to the latest available version.

Connection Properties

Connection properties manage streaming video performance over remote connections to target servers.

The properties are applied only to your connection - they do not impact the connection of other users accessing the same target servers.

If you make changes to connection properties, they are retained by the client.

► To view connection properties:

- Choose File > Connection Properties.

Default Connection Properties

The KX III comes configured to provide optimal performance for the majority of video streaming conditions.

Default connection settings are:

- Optimized for: Text Readability - video modes are designed to maximize text readability.
This setting is ideal for general IT and computer applications, such as performing server administration.
- Video Mode - defaults to Full Color 2.
Video frames transmit in high-quality, 24-bit color. This setting is suitable where a high-speed LAN is used.
- Noise Filter - defaults to 2.
The noise filter setting does not often need to be changed.

Click Reset to regain the default connection properties.

Connection Properties

Optimize for: Text Readability ▼

Video Mode: Full Color 2

Best Quality

Noise Filter: 2

Lower Bandwidth

Reset

OK

Cancel

Apply

Text Readability

Text Readability is designed to provide video modes with lower color depth but text remains readable. Greyscale modes are even available when applying lower bandwidth settings.

This setting is ideal when working with computer GUIs, such as server administration.

When working in full color video modes, a slight contrast boost is provided, and text is sharper.

In lower quality video modes, bandwidth is decreased at the expense of accuracy.

Color Accuracy

When Color Accuracy is selected, all video modes are rendered in full 24-bit color with more compression artifacts.

This setting applies to viewing video streams such as movies or other broadcast streams.

In lower quality video modes, sharpness of fine detail, such as text, is sacrificed.

Video Mode

The Video Mode slider controls each video frame's encoding, affecting video quality, frame rate and bandwidth.

Connection Properties

Optimize for:
Text Readability ▼

Video Mode: Full Color 2

Best Quality

Noise Filter: 2

Lower Bandwidth

Reset
OK
Cancel
Apply

In general, moving the slider to the left results in higher quality at the cost of higher bandwidth and, in some cases, lower frame rate.

Moving the slider to the right enables stronger compression, reducing the bandwidth per frame, but video quality is reduced.

In situations where system bandwidth is a limiting factor, moving the video mode slider to the right can result in higher frame rates.

When Text Readability is selected as the Optimized setting, the four rightmost modes provide reduced color resolution or no color at all.

These modes are appropriate for administration work where text and GUI elements take priority, and bandwidth is at a premium.

Noise Filter

Unless there is a specific need to do so, do not change the noise filter setting. The default setting is designed to work well in most situations.

The Noise Filter controls how much interframe noise is absorbed by the KX III.

Connection Properties

Optimize for: Text Readability ▾

Video Mode: Full Color 2

Best Quality

Noise Filter: 2

Lower Bandwidth

Reset OK Cancel Apply

Moving the Noise Filter slider to the left lowers the filter threshold, resulting in higher dynamic video quality. However, more noise is likely to come through, resulting in higher bandwidth and lower frame rates.

Moving the slider to the right raises the threshold, allows less noise and less bandwidth is used. Video artifacts may be increased.

Moving the noise filter to the right may be useful when accessing a computer GUI over severely bandwidth-limited connections.

Connection Info

Open the Connection Information dialog for real-time connection information on your current connection, and copy the information from the dialog as needed.

See **Connection Properties** (see "**Default Connection Properties**" on page 307) for help configuring the connection properties.

- Name of the KX III
- IP address of the KX III
- Port - The KVM communication TCP/IP port used to access KX III.
- Data In/Second - Data rate received from the KX III
- Data Out/Second - Data rate sent to the KX III.
- FPS - Video frames per second from the KX III.
- Average FPS - Average number of video frames per second.
- Connect Time - The duration of the current connection.
- Horizontal Resolution - The target server horizontal resolution.
- Vertical Resolution - The target server vertical resolution.
- Refresh Rate - Refresh rate of the target server.
- Protocol Version - Raritan communications protocol version.

► To view connection info:

- Choose File > Connection Info.

Connection Info

Device Name:	kx3-61-16
IP Address:	192.168.61.16
Port:	443
Data In/Second:	121 kB/s
Data Out/Second:	234 B/s
FPS:	17
Avg. FPS:	21.80
Connect Time:	00:00:25
Horizontal Resolution:	1024
Vertical Resolution:	768
Refresh Rate:	60 Hz
Protocol Version:	1.31

OK

USB Profile

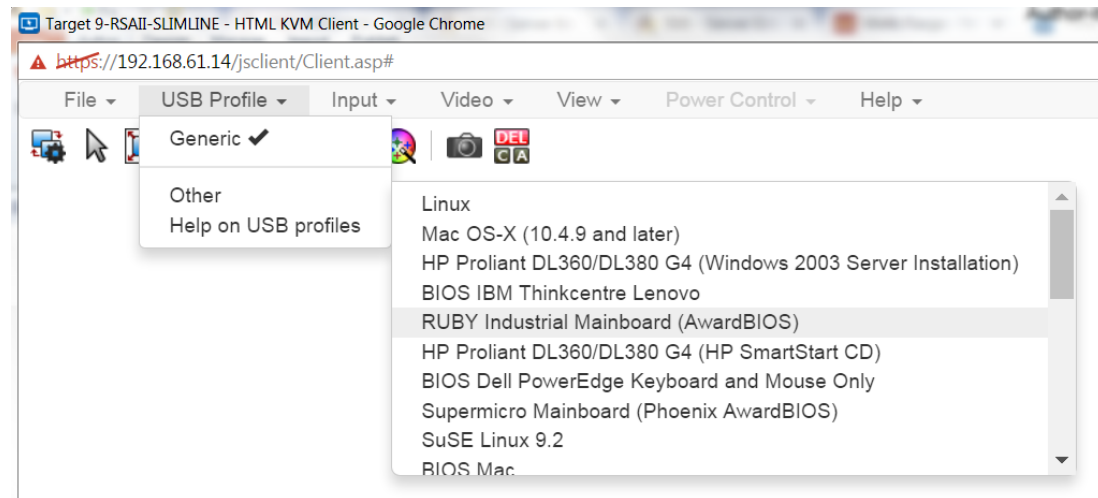
Select a USB profile that best applies to the KVM target server.

For example, if the server is running Windows® operating system, it would be best to use the Generic profile.

Or, to change settings in the BIOS menu or boot from a virtual media drive, depending on the target server model, a BIOS profile may be more appropriate.

► To set a USB profile for a target server:

- Choose USB Profile, then choose Generic, or choose Other Profiles to select from a menu.



► To view details on USB profiles:

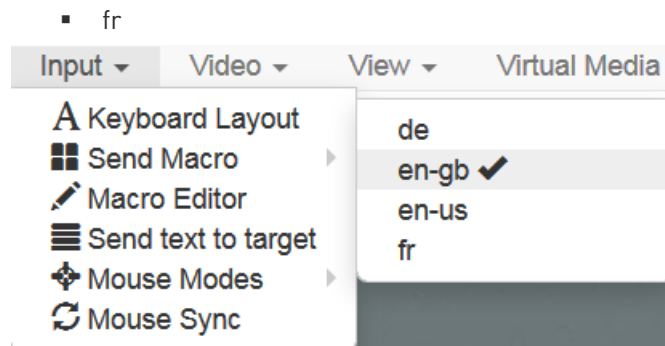
Choose USB Profile > Help on USB Profiles.

Input Menu

Keyboard Layout

► To set your keyboard type.

- Choose Input > Keyboard Layout, then select your keyboard type.
 - de
 - en-gb
 - en-us

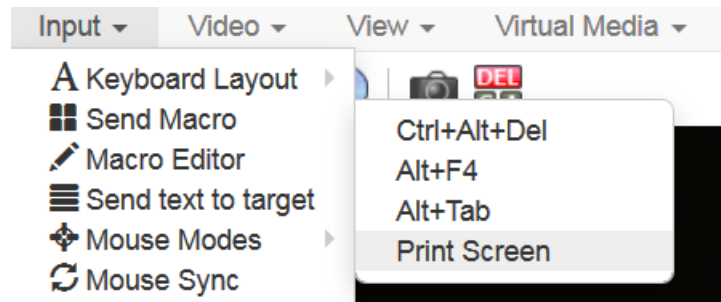


Send Macro

Due to frequent use, several keyboard macros are preprogrammed.

► **To send a preprogrammed macro:**

- Choose Input > Send Macro, then select the macro:
 - Ctrl+Alt+Del: Sends the key sequence to the target without affecting the client.
 - Alt+F4: Closes a window on a target server.
 - Alt+Tab: Switch between open windows on a target server.
 - Print Screen: Take a screenshot of the target server.



Macro Editor

Keyboard macros ensure that keystroke combinations intended for the target server are sent to and interpreted only by the target server. Otherwise, they might be interpreted by your client PC.

Macros are stored on the client PC and are PC-specific. If you use another PC, you cannot see your macros.

In addition, if another person uses your PC and logs in under a different name, that user will see your macros since they are computer-wide.

Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one KX3 device, your macros will only be available on the browser and KX3 device where they were created. To reuse your macros in another KX3 device, you can import and export the macro files. See *Import and Export Macros* (on page 316).

► **To access the Macro Editor:**

- Choose Inputs > Macro Editor.
- Select a macro from the Macros list to view the key combination.

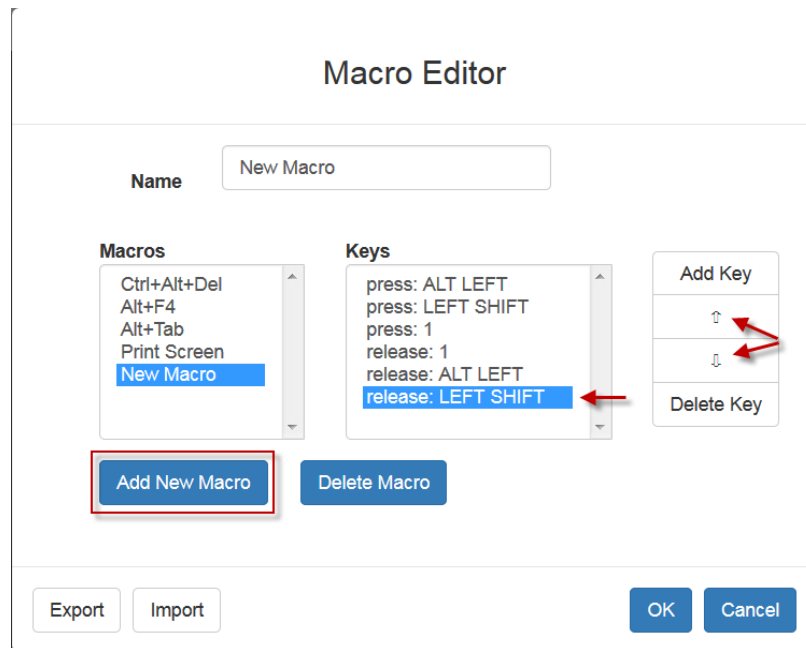
Macro Editor

Add New Macro

► **To add a new macro:**

1. Choose Inputs > Macro Editor.
2. Click Add New Macro.

3. Enter a Name for the new macro. The name will appear in the Send Macro menu once the macro is saved.
4. Click Add Key, then press the key you want to add to the macro. The key press and key release appear in the Keys list.
 - To add more keys, click Add Key again, and press another key.
 - To remove a key, select it in the Keys list and click Delete Key
5. To put the key in the correct sequence, click to select a key in the Keys list, then click the up and down arrows.
6. Click OK to save.



Delete a Macro

► To delete a macro:

1. Choose Inputs > Macro Editor.
2. Select the macro, then click Delete Macro.

- Click OK.

Macro Editor

Name

Macros

Ctrl+Alt+Del
 Alt+F4
 Alt+Tab
 Print Screen
 New Macro

Add New Macro
Delete Macro

Keys

press: ALT LEFT
 press: LEFT SHIFT
 press: 1
 release: 1
 release: ALT LEFT
 release: LEFT SHIFT

Add Key
Delete Key

Add Key

↑

↓

Delete Key

Export **Import**

OK **Cancel**

Import and Export Macros

Macros created with HKC are only available with the current browser and KVM device. If you use HKC in more than one browser, or more than one KX3 device, your macros will only be available on the browser and KX3 device where they were created. To reuse your macros in another KX3 device, you can import and export the macro files. Imported and exported macro files created on HKC are only compatible with HKC, and cannot be used on AKC or VKC. Likewise, macro files created on AKC or VKC cannot be imported for use on HKC.

Macros are exported to an xml file named "usermacros.xml". Files are saved in your browser's default download location. Default macros are not exported.

► To export and import macros:

- Choose Input > Macro Editor. The list of macros created for your browser and KX3 device displays in the Macro Editor dialog.
- To export the list, click the Export button, then save the file.
- Log in to the KX3 device where you want to import the macros.
- Choose Input > Macro Editor.
- Click Import, then click Open to Import and select the usermacros.xml file, and click OK.
- The macros found in the file display in the list. Select the macros you want to import, then click OK.

- Macro names must be unique. If a macro with the same name already exists, an error message appears. Click the Edit icon to rename the macro, then click the checkmark to save the name.

Macro Import

Open to Import

Select macros to import:

Macro1

✎

Select All

Deselect All

OK

Cancel

Send Text to Target

Use the Send Text to Target function to send text directly to the target. If a text editor or command prompt is open and selected on the target, the text is pasted there.

► To send text to target:

1. Choose Input > Send Text to Target. The Send Text to Target dialog appears.
2. Enter the text you want sent to the target. Supported keyboard characters only.
3. Click OK.

Mouse Modes

You can operate in either single mouse mode or dual mouse mode.

When in a dual mouse mode, and provided the option is properly configured, the mouse cursors align.

When controlling a target server, the Remote Console displays two mouse cursors - one belonging to your KX III client workstation, and the other belonging to the target server.

When there are two mouse cursors, the device offers several mouse modes:

- Absolute (Mouse Synchronization)
- Intelligent (Mouse Mode)
- Standard (Mouse Mode)

When the mouse pointer lies within the KVM Client target server window, mouse movements and clicks are directly transmitted to the connected target server.

While in motion, the client mouse pointer slightly leads the target mouse pointer due to mouse acceleration settings.

On fast LAN connections, you can use single mouse mode, and view only the target server's pointer.

You can toggle between these two modes (single mouse and dual mouse).

Absolute Mouse Synchronization

In this mode, absolute coordinates are used to keep the client and target cursors in synch, even when the target mouse is set to a different acceleration or speed.

This mode is supported on servers with USB ports and is the default mode for virtual media CIMs.

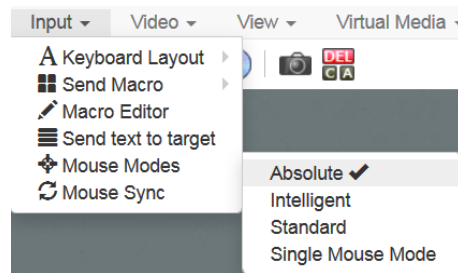
Absolute Mouse Synchronization requires the use of a virtual media CIM

-

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

► **To enter Absolute Mouse Synchronization Mode:**

- Choose Input > Mouse Modes > Absolute.

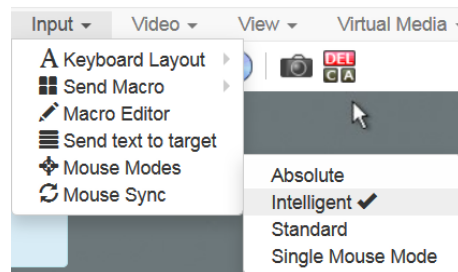


Intelligent

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target. Intelligent mouse mode is the default for non-VM targets.

► **To enter Intelligent mouse mode:**

- Choose Input > Mouse Mode > Intelligent. The mouse will synch. See ***Intelligent Mouse Synchronization Conditions*** (on page 276).



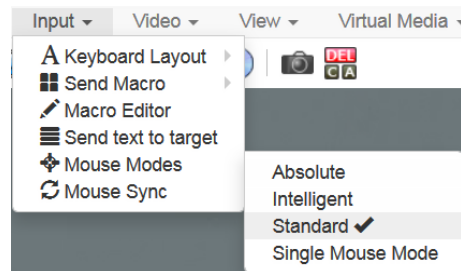
Standard

Standard Mouse mode uses a standard mouse synchronization algorithm. The algorithm determines relative mouse positions on the client and target server.

In order for the client and target mouse cursors to stay in synch, mouse acceleration must be disabled. Additionally, specific mouse parameters must be set correctly.

► **To enter Standard mouse mode:**

- Choose Input > Mouse Modes > Standard.

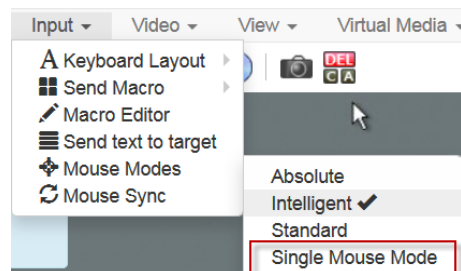
**Single**

Single Mouse mode uses only the target server mouse cursor; the client mouse cursor no longer appears onscreen.

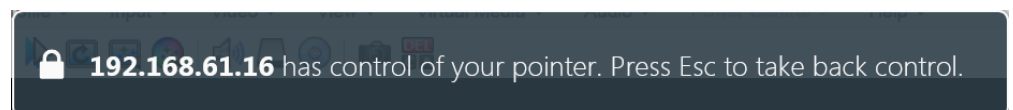
Note: Single mouse mode does not work on Windows or Linux targets when the client is running on a Virtual Machine.

► **To enter Single mouse mode:**

- Choose Inputs > Mouse Modes > Single.



- A message appears at the top of the client window: Press Esc to show your cursor.



► **To exit Single mouse mode:**

- Press Esc.
- Mouse mode changes back to dual mode.

Mouse Sync

In dual mouse mode, the Synchronize Mouse command forces realignment of the target server mouse cursor with the client mouse cursor.

Note: This option is available only in Standard and Intelligent mouse modes.

► **To synchronize the mouse cursors:**

- Choose Inputs > Mouse Sync.

Intelligent Mouse Synchronization Conditions

The Intelligent Mouse Synchronization command, available on the Mouse menu, automatically synchronizes mouse cursors during moments of inactivity. For this to work properly, however, the following conditions must be met:

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- Advanced mouse properties such as “Enhanced pointer precision” or “Snap mouse to default button in dialogs” should be disabled.
- Choose “Best Possible Video Mode” in the Video Settings window.
- The edges of the target video should be clearly visible (that is, a black border should be visible between the target desktop and the remote KVM console window when you scroll to an edge of the target video image).
- When using the intelligent mouse synchronization function, having a file icon or folder icon located in the upper left corner of your desktop may cause the function not to work properly. To be sure to avoid any problems with this function, Raritan recommends you do not have file icons or folder icons in the upper left corner of your desktop.

After autosensing the target video, manually initiate mouse synchronization by clicking the Synchronize Mouse button on the toolbar. This also applies when the resolution of the target changes if the mouse cursors start to desync from each other.

If intelligent mouse synchronization fails, this mode will revert to standard mouse synchronization behavior.

Please note that mouse configurations will vary on different target operating systems. Consult your OS guidelines for further details. Also note that intelligent mouse synchronization does not work with UNIX targets.

Video Menu

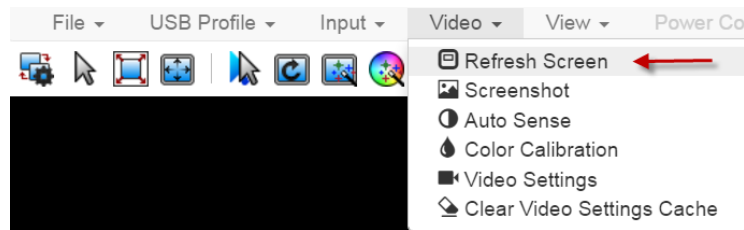
Refresh Screen

The Refresh Screen command forces a refresh of the video screen. Video settings can be refreshed automatically in several ways:

- The Refresh Screen command forces a refresh of the video screen.
- The Auto-Sense command automatically detects the target server's video settings.
- The Color Calibration command calibrates the video to enhance the colors being displayed.
- In addition, you can manually adjust the settings using the Video Settings command.

► To force a refresh of the video screen:

- Choose Video > Refresh Video.



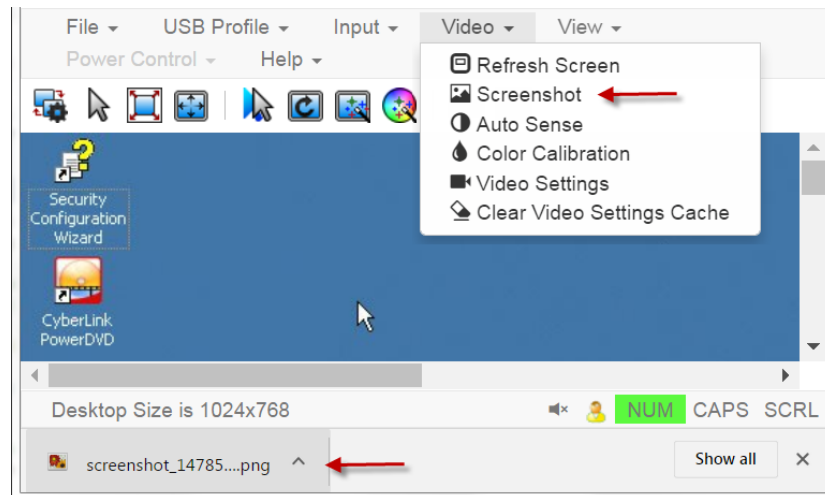
Screenshot

Take a screenshot of a target server using the Screenshot command.

► To take a screenshot of the target server:

1. Choose Video > Screenshot.

2. The screenshot file appears as a download to view or save. Exact options depend on your client browser.



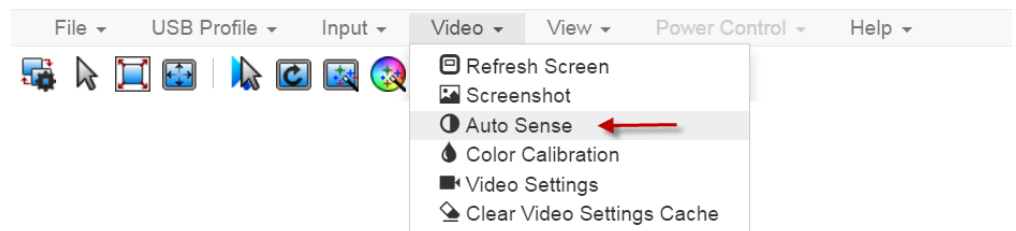
Auto Sense

The Auto Sense command forces a re-sensing of the video settings, such as resolution and refresh rate, and redraws the video screen.

► To automatically re-sense the video settings:

- Choose Video > Auto Sense .

A message stating that the auto adjustment is in progress appears.



Color Calibration

The Color Calibration command optimizes the color levels, such as hue, brightness, and saturation, of the transmitted video images.

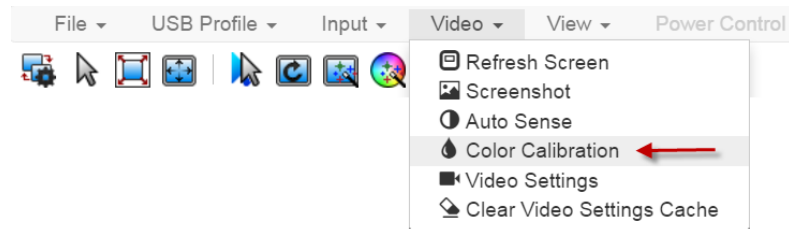
The color settings are on a target server-basis.

Note: When color is successfully calibrated, the values are cached and reused each time you switch to the target. Changes to the brightness and contrast in Video Settings are not cached. Changing resolution resets the video to the cached values again. You can clear the cached values in Video > Clear Video Settings Cache. See ***Clear Video Settings Cache*** (on page 271).

► To calibrate color:

- Choose Video > Color Calibration.

A message stating that the color calibration is in progress appears.



Video Settings

Use the Video Settings command to manually adjust the video settings.

► To change the video settings:

1. Choose Video > Video Settings to open the Video Settings dialog.
2. Adjust the following settings as required. As you adjust the settings the effects are immediately visible:
 - a. PLL Settings

Clock - Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended. Under most circumstances, this setting should not be changed because the autodetect is usually quite accurate.

Phase - Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.
 - b. Brightness: Use this setting to adjust the brightness of the target server display.

- c. Brightness Red - Controls the brightness of the target server display for the red signal.
- d. Brightness Green - Controls the brightness of the green signal.
- e. Brightness Blue - Controls the brightness of the blue signal.
- f. Contrast Red - Controls the red signal contrast.
- g. Contrast Green - Controls the green signal.
- h. Contrast Blue - Controls the blue signal.

If the video image looks extremely blurry or unfocused, the settings for clock and phase can be adjusted until a better image appears on the active target server.

Warning: Exercise caution when changing the Clock and Phase settings. Doing so may result in lost or distorted video and you may not be able to return to the previous state. Contact Raritan Technical Support before making any changes.

- i. Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor.

- j. Vertical Offset - Controls the vertical positioning of the target server display on your monitor.

Video Settings

PLL Settings

Clock

1344

1026

1844

Phase

20

0

31

Color Settings

Brightness Red

0

0

127

Brightness Green

0

0

127

Brightness Blue

0

0

127

Contrast Red

65

0

127

Contrast Green

69

0

127

Contrast Blue

70

0

127

Horizontal Offset

288

0

255

Vertical Offset

35

0

-768

☒ Automatic Color Calibration

Video Sensing

☒ Best possible video mode

☐ Quick sense video mode

OK

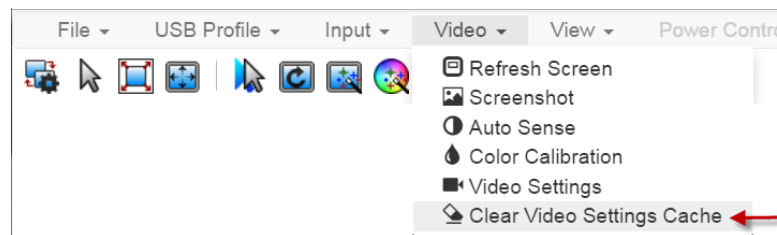
Cancel

Clear Video Settings Cache

You can clear the video settings cache to delete old settings that do not apply anymore, such as when a target server is replaced. When you clear the video settings cache, the server automatically does a video auto-sense and color calibration. The new values are cached and reused when the target is accessed again.

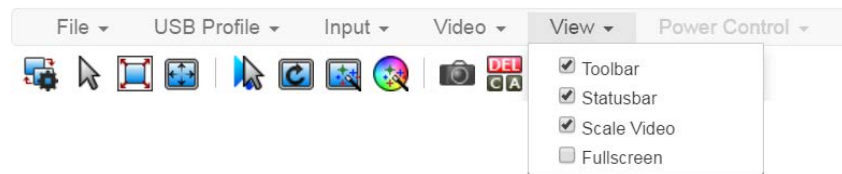
► To clear the video settings cache:

- Choose Video > Clear Video Settings Cache in the toolbar.



View Menu

The View Menu contains options to customize your HKC display.



► Toolbar and Statusbar:

The toolbar contains icons for some commands. The Statusbar displays screen resolution at the bottom of the client window.

► Scale Video:

Scale Video scales your video to view the entire contents of the target server window in your HKC window. The scaling maintains the aspect ratio so that you see the entire target server desktop without using the scroll bar.

► Fullscreen:

Fullscreen sets the target window to the size of your full screen, removing your client from the view.

- Press Esc to exit fullscreen.

Virtual Media Menu

Due to browser resources, virtual media file transfer is slower on HKC than the other KVM clients.

Connect Files and Folders

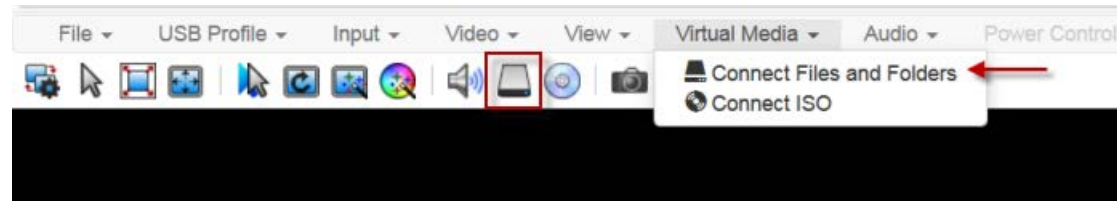
The Connect Files and Folders command provides an area to drag and drop files or folders that you want to connect to on virtual media.

Supported browsers: Chrome and Firefox

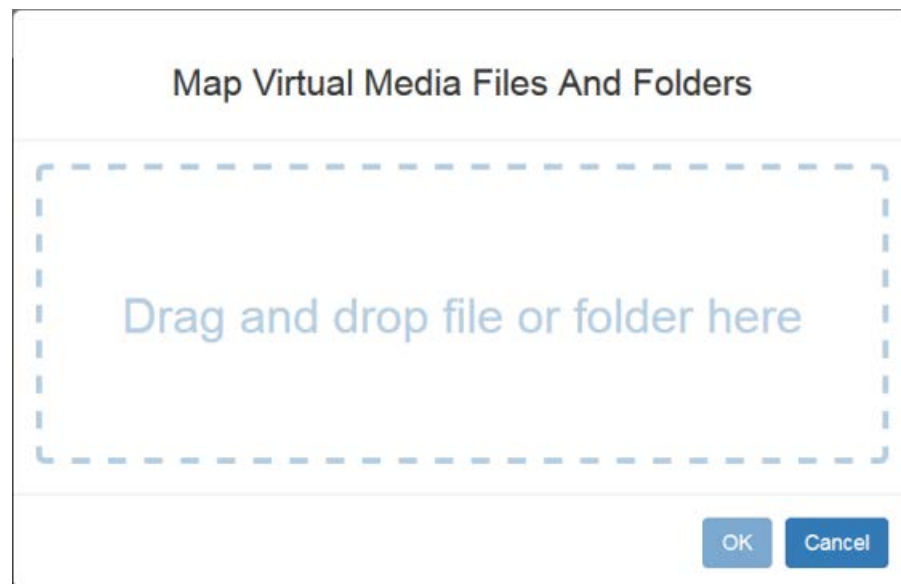
File size limit: 4GB per file

► To connect files and folders:

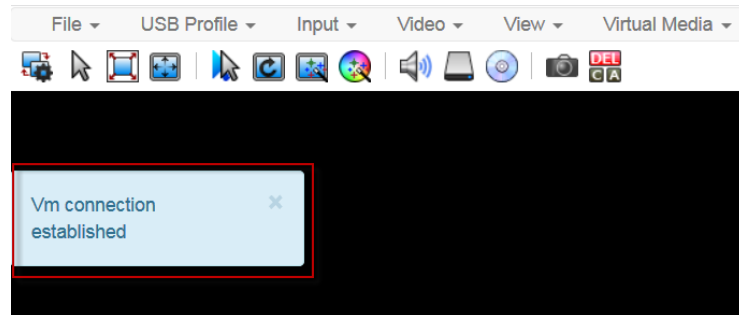
1. Choose Virtual Media > Connect Files and Folders. Or, click the matching icon in toolbar.



2. Drag files or folders onto the Map Virtual Media Files and Folders dialog. Click OK.



3. A message appears to show virtual media is connected. After a short time, a VM drive containing the selected files or folders will be mapped to the target server.



► **To disconnect files and folders:**

- Choose Virtual Media > Disconnect Files and Folders. Or, click the matching icon in the toolbar.



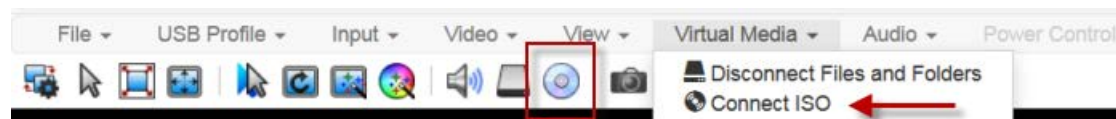
Connect ISO

The Connect ISO command maps a virtual media ISO image to the target. You can connect to ISO images on your client or on remote servers.

File size limit: 4GB per file

► **To map virtual media ISO images:**

1. Choose Virtual Media > Connect ISO. Or, click the matching icon in the toolbar.



2. Select the option for your file's location:

Map Virtual Media ISO Image

☒ **ISO Image** 

No file selected.

☐ **Remote Server ISO Image** 

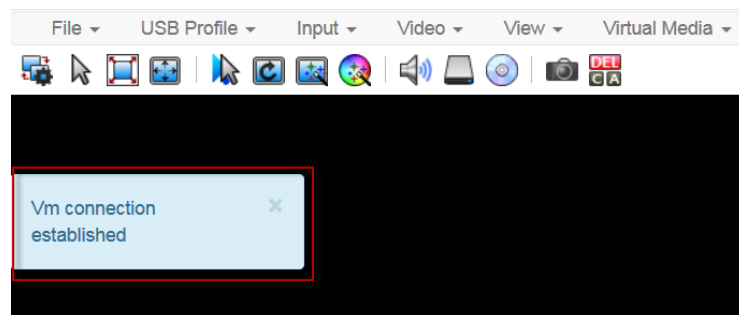
- Select ISO Image if the ISO file is directly accessible on your client. Click Browse, select the ISO file, and click OK. The filename appears next to the Browse button.

☒ **ISO Image**

Raritan.iso

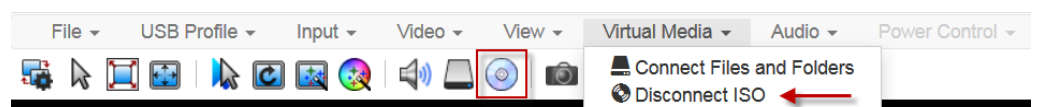
- Select Remote Server ISO Image if your ISO file is on a remote server. Remote ISO files must be pre-configured by an administrator for the mapping to appear here. See *Virtual Media File Server Setup (File Server ISO Images Only)* (on page 253). Select the Hostname, then select the ISO file from the Image list. Enter the file server's username and password.

3. Click OK to map the selected file to the target. A message appears to show virtual media is connected.



► **To disconnect ISO:**

- Choose Virtual Media > Disconnect ISO. Or, click the matching icon in the toolbar.



Audio Menu

The Audio menu contains audio connection and settings.

Note: IE does not support audio. The menu will appear grayed out.

Connect Audio

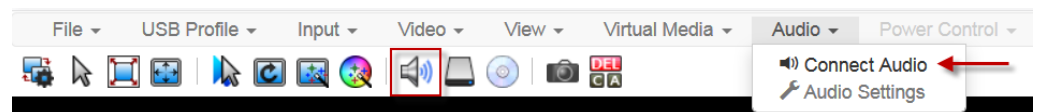
The Connect Audio command connects your playback device, selects audio format and gives an option to mount the selected playback device automatically when you connect to the target.

HKC connects the client PC's default audio playback device. To use a different device, it must be set as default in the client OS.

Note: For best quality, limit the number of audio sessions to a maximum of four KVM sessions.

► To connect audio:

1. Choose Audio > Connect Audio, or click the matching icon in the toolbar.



2. In the Connect Audio Device dialog, select the Connect Playback Device checkbox.

Connect Audio Device

☒ **Connect Playback Device**

Format:

stereo, 16bit, 44.100 Hz ▼

☐ **Mount selected playback device automatically on connection to target**

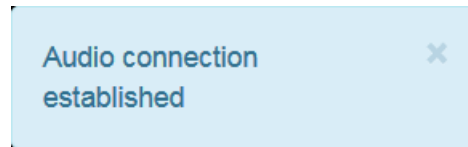
OK

Cancel

3. Select the Format:

stereo, 16bit, 44.100 Hz
 mono, 16bit, 44.100 Hz
 stereo, 16bit, 22.050 Hz
 mono, 16bit, 22.050 Hz
 stereo, 16bit, 11.025 Hz
 mono, 16bit, 11.025 Hz

4. Select the "Mount selected playback device automatically on connection to target" checkbox to enable the option. This setting will connect audio automatically the next time you connect to targets on the KX3.
5. Click OK. A success message appears.



► To disconnect audio:

1. Choose Audio > Disconnect Audio, or click the matching icon in the toolbar.

Audio Settings

The Audio Settings command is enabled when audio is connected. Use the Audio Settings to set the buffer and volume.

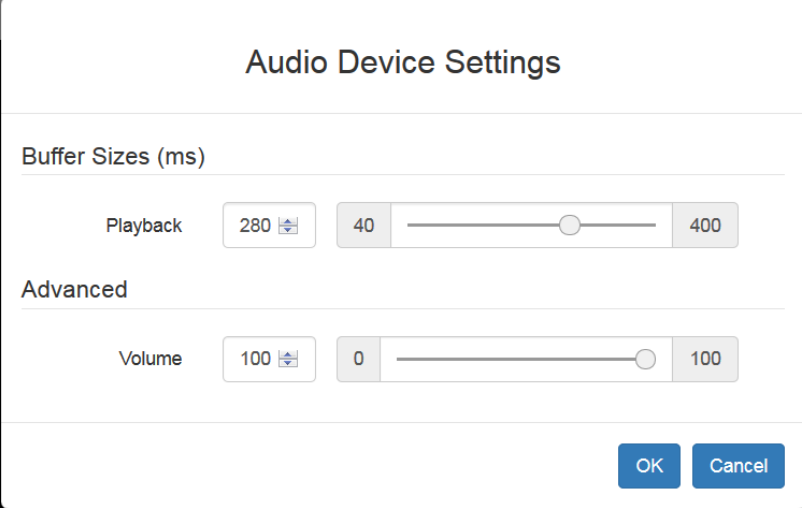
Increasing the buffer size improves the audio quality but may impact the delivery speed.

The maximum available buffer size is 400 milliseconds since anything higher than that greatly impacts audio quality.

► To configure audio settings:

1. Choose Audio > Audio Settings while Audio is connected.

2. Set the Buffer and Volume using the arrows or sliders.



The image shows a dialog box titled "Audio Device Settings". It has two sections: "Buffer Sizes (ms)" and "Advanced". In the "Buffer Sizes (ms)" section, there is a "Playback" label, a text box with "280" and a small icon, a slider with "40" on the left and "400" on the right, and a value of "40" is shown next to the slider. In the "Advanced" section, there is a "Volume" label, a text box with "100" and a small icon, a slider with "0" on the left and "100" on the right, and a value of "0" is shown next to the slider. At the bottom right, there are two buttons: "OK" and "Cancel".

3. Click OK.

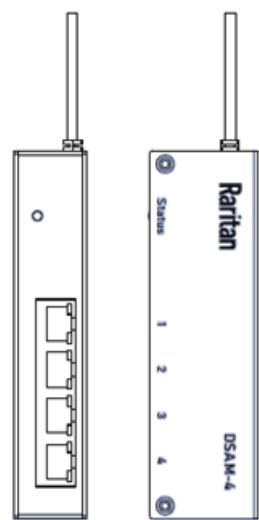
Power Control Menu

You can power on, power off, and power cycle a target through the outlet it is connected to.

Access the target, and then select a power control option from the Power Control menu.

The menu option is disabled if you do not have permission for power control, and when outlets are not associated with the port.

Chapter 6 Serial Access With Dominion Serial Access Module



Connecting a KX III and a Dominion Serial Access Module (DSAM) provides serial access for the KX III.

The DSAM is a 2- or 4 port serial module that derives power from the KX III.

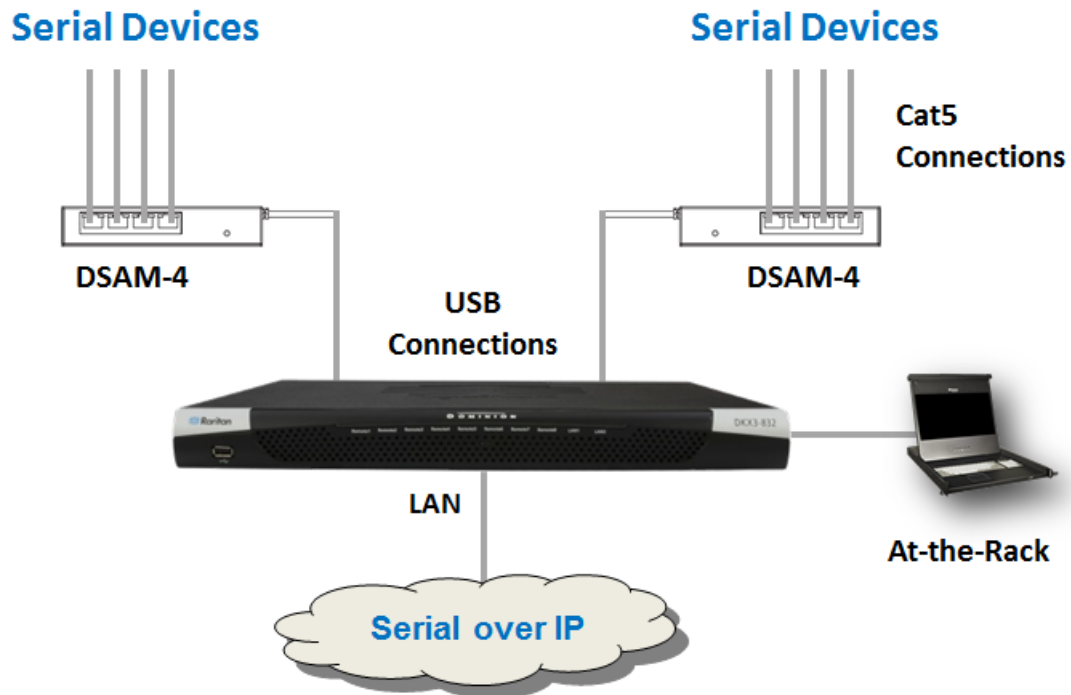
Connect a maximum of 2 DSAM modules to the KX III using USB cables. DSAM can be mounted in a 0U configuration.

In This Chapter

Connect KX III and DSAM	336
View DSAM Serial Ports	338
Configure DSAM Serial Ports	338
Configure Serial Port Keyword List	342
Upgrade DSAM Firmware	342
Supported CLI Commands	344
Connect to DSAM Serial Targets with KX3 GUI	348
Connect to DSAM Serial Target with URL Direct Port Access	349
Connect to DSAM Serial Target via SSH	350
HTML Serial Console (HSC) Help	351

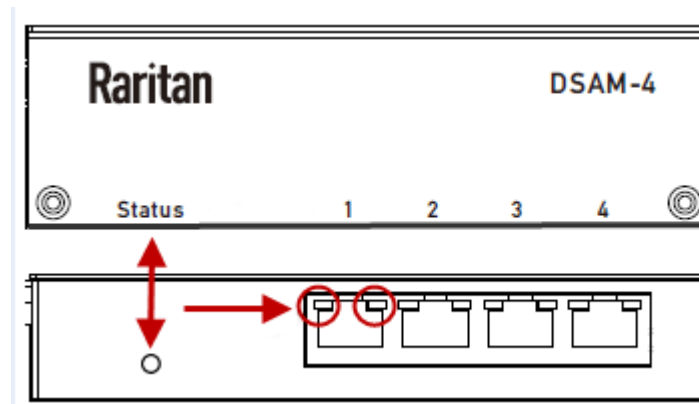
Connect KX III and DSAM

1. Connect the DSAM unit's USB cable to any USB port on the KX III device.
2. Connect the serial devices to the serial ports on the DSAM unit.



DSAM LED Operation

The DSAM unit has one LED for status, and 2 LEDs on each port.



► Status LED:

The Status LED is labeled on the unit front. Light is on back. The Status LED gives information at bootup and upgrade.

- Green LED - Slow blink: DSAM booting up but not controlled by KX3.
- Blue LED - Slow blink: DSAM controlled by KX3.
- Blue LED - Fast blink: Firmware upgrade in progress.

► USB Port LEDs:

Each USB port has a left Blue LED and a right Yellow LED.

- Blue LED: Port is set as DCE
- Yellow LED: Port is set as DTE
- LEDs off: Port is set as AUTO

Supported USB Device Combinations

Each USB device draws from a fixed pool of USB resources. There are limits on the number of USB devices that can be connected to the KX III at the same time.

The following device combinations are supported.

Device	C1	C2	C3	C4	C5
4-Port DSAM	X			X	
4-Port DSAM	X	X	X		
2-Port DSAM		X	X		X
2-Port DSAM					
Keyboard and Mouse		X		X	X
SmartCard				X	X
Wireless Modem			X	X	X
DSAM Ports	8	6	6	4	2

View DSAM Serial Ports

When a DSAM unit is connected to KX III, a new tab is available in the Ports page. The View by Serial tab shows all connected serial ports.

Port Access Power Virtual Media User Management Device Settings Security Maintenance Diag

Home > Ports

Port Access

*Click on the individual port name to see allowable operations.
0 / 1 Remote KVM channels currently in use.*

View By ~~Port~~ View By Serial View By Group View By Search Set Scan

▲ No.	Name	USB Port	Type	Status	Availability
4	DSAM4	Front	DSAM	up	
4.1	DSAM4 Port 1		DCE	up	idle
4.2	DSAM4 Port 2		AUTO	down	idle
4.3	DSAM4 Port 3		AUTO	down	idle
4.4	DSAM4 Port 4		AUTO	down	idle

32 Rows per Page [Set](#)

► To view DSAM serial ports:

In the Port Access page, click the View By Serial tab.

- Ports are listed by physical USB position on the DSAM unit.
- USB Port column indicates which KX III USB port DSAM is plugged into.
- Type column indicates port's DTE/DCE setting.

Configure DSAM Serial Ports

The serial port configuration options are available when a DSAM unit is connected to KX III using a USB port.

► To configure DSAM serial ports:

1. Choose Device Settings > Serial Port Configuration.
2. Click the Port Name for the port you want to configure.

Port Access Power Virtual Media User Management Device Settings

Home > Device Settings > Serial Port Configuration

Serial Port Configuration

▲ No.	Name	Type
4.1	DSAM4 Port 1	DCE
4.2	DSAM4 Port 2	AUTO
4.3	DSAM4 Port 3	AUTO
4.4	DSAM4 Port 4	AUTO

3. The Port Type is set to Serial only.
4. Enter a meaningful name for the serial target or leave the default name.

Port 4.1

Type:

Serial

Name:

DSAM4 Port 1

Power Association

If an outlet is connected to the same server that the port is connected to, a power association can be made with the target device.

A port can have up to four associated outlets, and you can associate a different rack PDU (power strip) with each. From this page, you can define those associations so that you can power on, power off, and power cycle the server from the Port Access page.

To use this feature, you need Raritan remote rack PDU(s).

1. Select the Power Strip Name and associate a name with each of the power strip's outlets by selecting from the Outlet Name drop-down.
2. Click OK. A confirmation message is displayed.

Power Association

Power Strip Name	Outlet Name
Powerstrip ▼	New outlet1 ▼
Powerstrip ▼	Outlet 2 ▼
Powerstrip ▼	Outlet 3 ▼
Powerstrip ▼	Outlet 4 ▼

Serial Port Settings

Configure the remaining port settings.

1. Select the terminal emulation type from the drop-down menu in the Emulation field. This is the terminal emulation mode used to match the serial targets connected to the ports.
 - VT100
 - VT220
 - VT320
 - ANSI
2. Set Encoding if you want to always use a specific character encoding for this port. Encoding overrides the global setting for the port to whatever value you set.
 - DEFAULT
 - US-ASCII

- ISO8859-1
 - ISO8859-15
 - UTF-8
 - Shift-JIS
 - EUC-JP
 - EUC-CN
 - EUC-KR
3. In the Equipment Type field, indicate whether you want the KX III to automatically detect a physical connection to the target. The default is Auto Detection.

Force DTE causes KX III to act as a piece of data terminal detection equipment to detect targets connected to it.

Force DCE causes KX III to act as a piece of data communications equipment to detect equipment connected to it.

Note: If the target has the ability to autodetect either DTE or DCE, you must select either Force DTE or Force DCE for the port. KX III does not support autodetection of both DCE and DTE on the same port.

4. Select the value of Bits Per Second from the Bits Per Second drop-down menu.
5. Select the Parity Bits from the Parity Bits drop-down menu.
6. Select the Flow Control from the Flow Control drop-down menu.
7. Stop Bits
8. If you need to configure the delay between when individual characters are sent via the port, enter the time in milliseconds in the Char Delay field.
9. To configure the delay between when lines of text are sent via the port, enter it in the Line Delay field.
10. Configure the sendbreak duration by entering the send break time in the Send Break Duration field. The send break is configurable from 0ms - 1000ms.
11. Select Always Active if you want to log activities coming into a port even if no user is connected.

The default option is to not maintain port access without a connected user, which means ignore data coming into a port when no user is connected.

This option is for port data logs.

Note: When no users are logged into a port session, port traffic, by default, is discarded .

12. If you do not want messages displayed to users connecting to KX III via Direct Port Access, select the Suppress Message checkbox.
13. Select the Escape Mode.

The escape sequence affects only the CLI. When entering the escape mode, the user is given a menu of commands that can be performed (for example, gethistory, power commands, and so on), a command to return to the port session, and a command to exit the port connection.

The default is None.

Change as follows:

 - Select control from the drop-down menu in the Escape Mode field.
14. Type the character in the Escape Character field. The default for the KX III is] (closed bracket).

Raritan recommends that you do not use [or Ctrl-[, Either of these may cause unintended commands, such as invoking the Escape Command unintentionally. This key sequence is also triggered by the arrow keys on the keyboard.
15. Type a command in the Exit Command field, such as logout.

This is the command that is sent to your system when a user with write permission disconnects from the port.

The main function of this command is to ensure that the user's session on the target machine is closed; however, it is not imperative to have an Exit command configured on a port.
16. Click OK.

Apply Settings to Other Ports

Once finished, you can apply the same port settings to other ports.

1. Select the ports from the Apply Serial Port Settings To Other Ports section of the page.
2. Click OK to apply the port configuration settings.

Configure Serial Port Keyword List

Port keywords work as a filter. You can create port keywords and associate them with -

- Events
- Local/remote syslog messages
- SNMP traps

If a keyword is detected -

- A corresponding message is logged in a local/NFS port log.
- A corresponding event is sent via SMTP (if configured).
- A corresponding trap is sent via SNMP (if configured).

This feature is useful for notifying administrators if a particular event occurs on a port. Using port keywords to report events does not impact the NFS log size.

For keywords to trigger when no users are connected to a port, "Always Active" must be selected on the port's Port Configuration page.

A list of existing port keywords is displayed on the Port Configuration page as well.

► **To configure serial port keywords:**

1. Choose Device Settings > Serial Port Keywords. The Serial Port Keyword List page opens.
2. Click Add at the bottom of list on the page. The Keyword page opens.
3. Type a keyword in the Keyword field.
4. Select the Port(s) you want to associate with that keyword.
5. Click Add to add them to the Selected box.
6. Click OK.

Upgrade DSAM Firmware

DSAM firmware is upgraded automatically during KX III device firmware upgrades if a new DSAM version is detected in the device firmware. You can also upgrade your DSAM firmware manually.

► **To upgrade the DSAM firmware manually:**

1. Choose Maintenance > DSAM Firmware Upgrade.

2. Select the checkboxes for the DSAM units you want to upgrade to the Upgrade DSAM Version listed.

DSAM Upgrade from Device Flash

DominionKX DSAMs:

Select All

Deselect All

Selected	Port	Name	USB Port	Current DSAM Version	Upgrade DSAM Version
☒	4	DSAM4	Front	0.21	0.22

Upgrade

Cancel

3. Click Upgrade, then click OK to confirm. A progress message appears.

Firmware Upgrade in Progress...

DSAMs on Device DominionKX are being upgraded. It may take up to 2 minutes to upgrade the selected DSAMs. Do not turn off the unit or remove DSAMs until the upgrade is complete.

Progress: 0 of 1 DSAMs upgraded

0%

4. When firmware upgrade completes, a success message appears.

Firmware Upgrade in Progress...

Upgrade of DSAM(s) on device, DominionKX , has completed. You will now be redirected to the Port Access page.

Ok

Progress: DSAM Upgrade Finished Successfully

100%

Port	Serial Number	Result
4	RKK6693758	Successful

Supported CLI Commands

Port Connect Commands

Connect to a serial port using port number or port name. Use double quotes around port names that contain space symbols. For example: "DSAM Port 1".

```
admin > connect <port number>
```

```
admin > connect <port name>
```

► **Port number example:**

```
admin > connect 1.1
```

► **Port name example:**

```
admin > connect "DSAM Port 1"
```

Port Sub-Menu Commands

The port sub-menu can be reached using the escape key sequence.

Clear history buffer for this port.

```
admin > [portname] > clearhistory
```

Close this target connection. When a target is disconnected, the appropriate disconnect message appears.

```
admin > [portname] > close, quit, q
```

Display the history buffer for this port.

```
admin > [portname] > gethistory
```

Get write access for the port.

```
admin > [portname] > getwrite
```

Return to the target session.

```
admin > [portname] > return
```

Send a break to the connected target.

```
admin > [portname] > sendbreak
```

Lock write access to this port.

```
admin > [portname] > writelock
```

Unlock write access to this port.

```
admin > [portname] > writeunlock
```

Query Power status of this port.

```
admin > [portname] > powerstatus
```

Toggle Power On/Off of this port.

```
admin > [portname] > powertoggle
```

Power on the target.

```
admin > [portname] > poweron
```

Power off the target.

```
admin > [portname] > poweroff
```

Power cycle the target.

```
admin > [portname] > powercycle
```

Configure Ports Commands

Enter `admin >` to access the menu.

Command	Description	Parameters
<code>listports</code>	List accessible ports	NA

Enter `admin > config > port` to access the menu.

Command	Description	Parameters
<code>keywordlist</code>	Display all configured keywords.	NA
<code>keywordadd</code>	Add a keyword to the port.	- port <number range *> - Single port or range of ports (1-n or 1,3,4 or * for all ports) - keyword <value> - When keyword is detected on target, notification is sent.
<code>keyworddelete</code>	Delete an existing keyword from the port.	- port <number range *> - Single port or range of ports (1-n or 1,3,4 or * for all ports) - keyword <value> - When keyword is detected on target, notification is sent.
<code>config port</code>		- port <number range *> - Single port or range of ports (1-n or 1,3,4 or * for all ports) - name <port name> - Port name - bps <1200 1800 2400 4800 9600 19200 38400 57600 115200 230400> - Port speed in bits-per-second

Command	Description	Parameters
		▪ parity <none even odd> - Port parity type ▪ flowcontrol <none hw sw> - Port flowcontrol type hw = hardware flow control sw =X on/X off) ▪ eqtype <auto dte dce> - Equipment type (auto=>AUTO Detection, dte=>Force DTE, dce=>Force DCE) ▪ Note: If the target has the ability to autodetect either DTE or DCE, you must select either Force DTE or Force DCE for the port. KX III does not support autodetection of both DCE and DTE on the same port. ▪ escapemode <none control> - Use Ctrl-key (escapemode=control) or single key (escapemode=none) as escape sequence; for example, Ctrl- => escapemode=control, escapechar= escapechar char-Escape character ▪ Raritan recommends that you do not use or Ctrl- as the Escape command. Either of these may cause unintended commands, such as opening a menu, instead of invoking the Escape Command. ▪ emulation <vt100 vt220 vt320 ansi> - Target Emulation type ▪ sendbreak <duration> - Duration of the sendbreak signal in milliseconds. ▪ exitstring <cmd #delay; > - Execute exit string when port session closes, for example, config port 1 exitstring logout (execute logout on exit) config port 1 exitstring #0 (disable exit string for the port). The delay is the amount of time to wait after writing the command to the target. Number in seconds up to 60. ▪ alwaysactive <true false> - Determine whether data coming into a port is logged, for example, config port 1 alwaysactive true (always log activities coming into a port even if no user is connected) config port 1 alwaysactive false (ignore data coming into

Command	Description	Parameters
		a port when no user is connected) ▪ suppress - Determine whether none or all messages should be displayed during a DPA connection, such as "Authentication successful" ▪ encoding - Target Encoding type (DEFAULT US-ASCII ISO-8859-1 ISO-8859-15 UTF-8 Shift-JIS EUC-JP EUC-CN EUC-KR) ▪ multiwrite - Port set in Multiple Writer Mode. ▪ chardelay delay - Delay inserted between writing characters (0-9999ms) ▪ linedelay delay - Delay inserted between writing lines (0-9999ms) ▪ stopbits - Number of bits used to signal the end of a character (usually 1) (1/2) ▪ stopbits <1/2> -Number of bits used to signal the end of a character ▪ chardelay - Delay inserted between characters (0-9999) in ms ▪ linedelay - Delay inserted between lines (0-9999) in ms ▪ escapechar - Escape character ▪ encoding - <DEFAULT/US-ASCII/ISO-8859-1/ISO-8859-15/UTF-8/Shift-JIS/EUC-JP/EUC-CN/EUC-KR> - Target encoding type ▪ multiwrite <true/false> - Port set in multiple writer mode ▪ suppress <true/false> - Suppress SX messages when connecting to this target(true/false) ▪ sendbreak - Duration of sendbreak signal in ms

Command Line Interface Shortcuts

- Press the Up arrow key to display the last entry.
- Press Backspace to delete the last character typed.
- Press Ctrl + C to terminate a command or cancel a command if you typed the wrong parameters.
- Press Enter on your keyboard to execute the command.
- Press Tab on your keyboard to complete a command. Tab also completes parameters and values (if the value is part of an enumerated set).

Command Line Interface High-Level Commands

The CLI is menu based. Some commands move to a menu with a different command set.

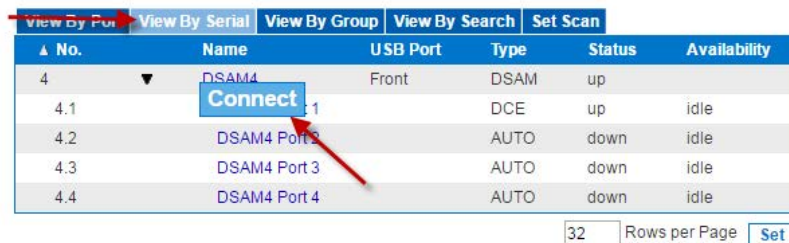
The following common commands can be used at all levels of the command line interface (CLI):

- **top** - Return to the top level of the CLI hierarchy, or the username prompt.
- **history** - Displays the last 200 commands the user entered into the KX III CLI.
- **logout** - Logs the user out of the current session.
- **quit** - Moves the user back one level in the CLI hierarchy.
- **help** - Displays an overview of the CLI syntax.

Connect to DSAM Serial Targets with KX3 GUI

► To connect to DSAM serial targets:

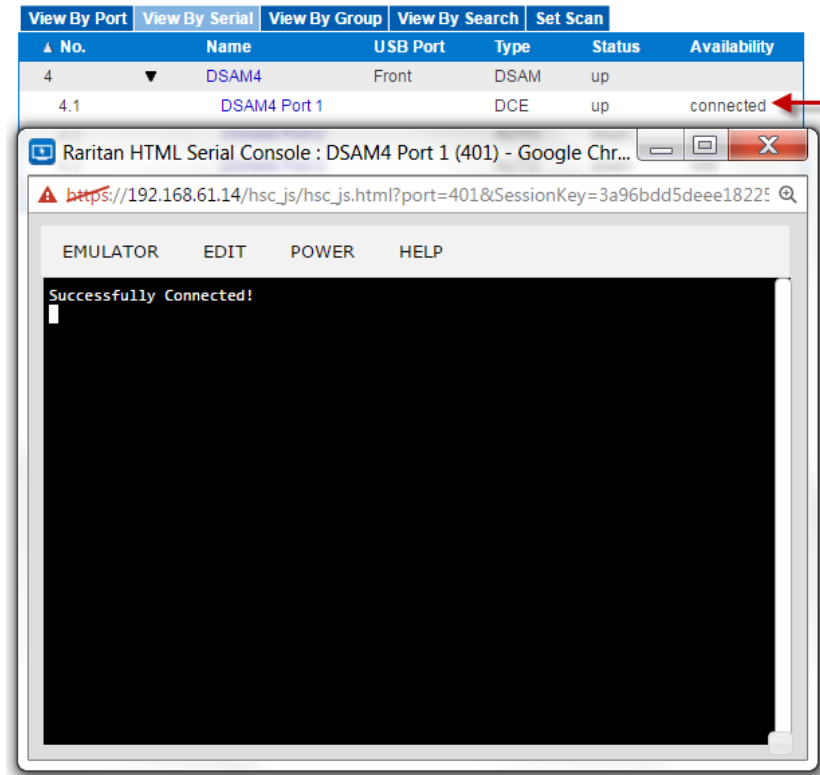
1. In the Port Access page, click the View By Serial tab to view the serial targets.
2. Click the port name you want to connect to. Click Connect.



▲ No.	Name	USB Port	Type	Status	Availability
4	DSAM4	Front	DSAM	up	
4.1	DSAM4 Port 1		DCE	up	idle
4.2	DSAM4 Port 2		AUTO	down	idle
4.3	DSAM4 Port 3		AUTO	down	idle
4.4	DSAM4 Port 4		AUTO	down	idle

32 Rows per Page

- The HTML Serial Console (HSC) window opens. See *HTML Serial Console* (see "*HTML Serial Console (HSC) Help*" on page 351)



- To exit the serial port, hit the hot-key. Default hot key is Scrolllock-Scrolllock.

Connect to DSAM Serial Target with URL Direct Port Access

- Choose Device Settings > Device Services, then select the Enable Direct Port Access via URL checkbox.
- To connect with direct port access, type the URL:
`"https://<KX3 IP Address>/dpa.asp?port=<serial port number>&username=<user name>&password=<password>"`

Example:

`https://192.168.51.101/dpa.asp?port=4.1&username=admin&password=raritan0`

- HTML Serial Client (HSC) launches and connects to the serial target.

Connect to DSAM Serial Target via SSH

1. Choose Device Settings > Device Services, then select the Enable SSH checkbox.
2. Launch SSH client in client PC to connect to KX3.
3. After login, user will enter CLI interface.
4. Type command "connect <serial port number>", or type command "connect <name of serial port>".

Example-1: connect 4.1

Example-2: connect "DSAM4 Port1"

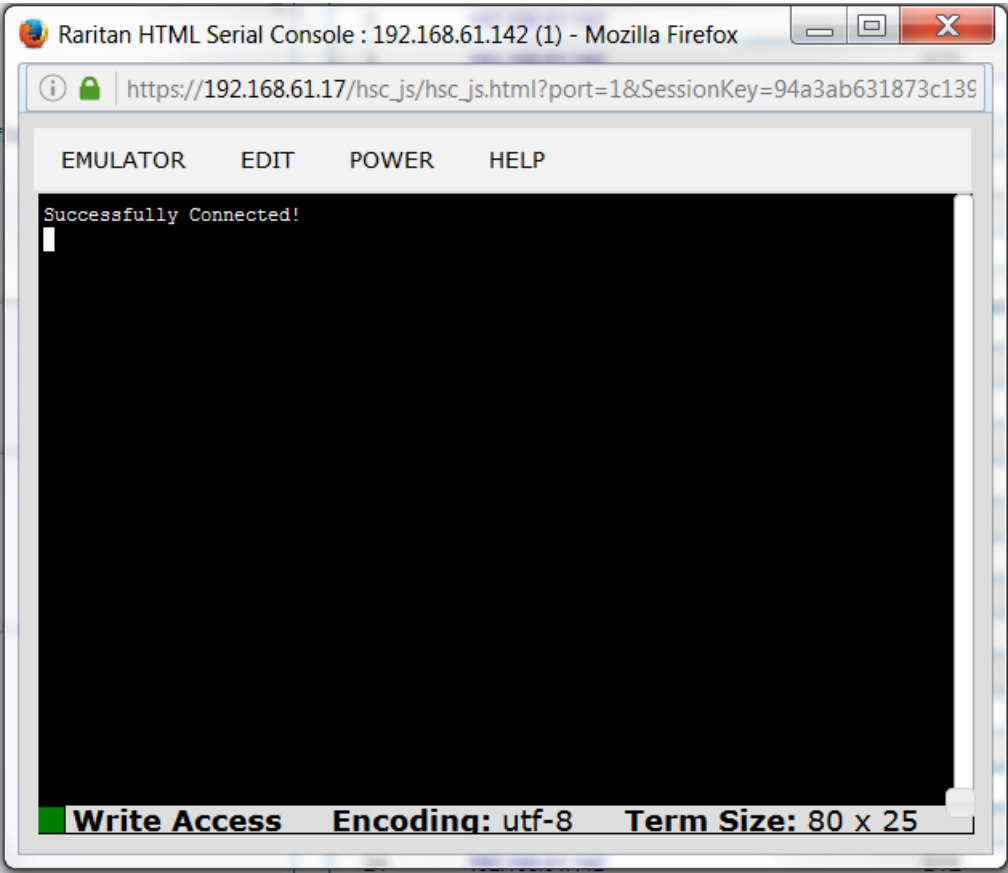
5. If successful, serial target is accessed.
6. To exit serial target, type escape-key-sequence, default is Ctrl-], then enter port sub-menu CLI interface.
7. Type "quit", then enter main CLI interface.

Chapter 7

HTML Serial Console (HSC) Help

Use HSC to connect to serial targets from SX II. HSC is also launched when accessing SX II targets in CC-SG. **Note:** HSC does not support CC-SG's proxy mode in release 6.2.

Note: You can also access targets via Direct Port Access, command line interface (CLI), local port GUI, and SSH.



In This Chapter

HSC Functions..... 352

HSC Functions

Emulator

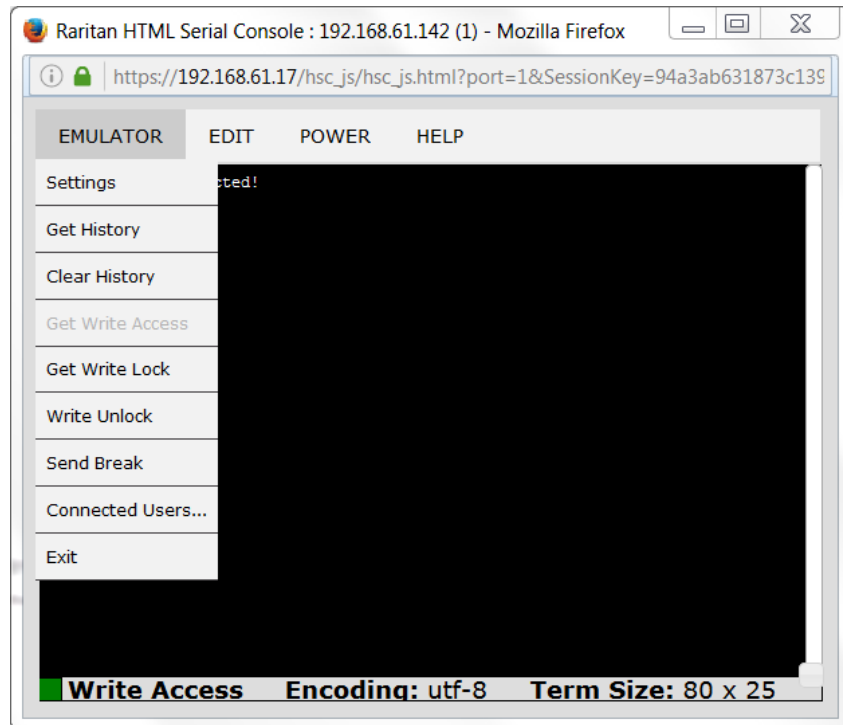
IMPORTANT: HSC sessions are affected by the KX III Idle Timeout.

If you have not changed the KX III Idle Timeout setting from the default, your session could be closed automatically if it exceeds the Idle Timeout period.

Change the default Idle Timeout setting and then launch the HSC. See Login Limitations for details on changing the Idle Timeout setting.

Access Emulator Options

1. Select the Emulator drop-down menu to display a list of options.



Settings

Note: An Administrator can set Terminal emulation settings using Setup > Port Configuration.

1. Choose Emulator > Settings. The Terminal Properties dialog displays the default settings.

Terminal Properties

Columns: 80 Rows: 25

Foreground: Background:

Font size: 11 Scrollback: 1000

Encoding: utf-8 Language: English

Backspace Sends: Ctrl-H

OK Cancel

2. Set the terminal size by selecting the number of Columns and Rows. Default is 80 by 25.
3. Set the Foreground and Background colors. Default is white on black.
4. Set the Font size. Default is 11.
5. Set the Scrollback number to indicate the number of lines available for scrolling.
6. Choose one of the following from the Encoding drop-down menu:
 - US-ASCII
 - ISO-8859-1
 - ISO-8859-15
 - UTF-8
 - Shift-JIS
 - EUC-JP
 - EUC-KR
7. Choose one of the following from the Language drop-down menu:
 - English
 - Japanese
 - Korean
 - Chinese
 - Bulgarian
8. The Backspace Sends default is ASCII DEL, or you can choose Control-H from the Backspace Sends drop-down menu.

9. Click OK to save. If you changed the Language setting, the HSC changes to that language when the Display Settings window is closed.

Get History

History information can be useful when debugging, troubleshooting, or administering a target device. The Get History feature:

- Allows you to view the recent history of console sessions by displaying the console messages to and from the target device.
- Displays up to 512KB of recent console message history. This allows a user to see target device events over time.

When the size limit is reached, the text wraps, overwriting the oldest data with the newest.

Notes: History data is displayed only to the user who requested the history.

To view the Session History, choose Emulator > Get History.

Clear History

- To clear the history, choose Emulator > Clear History.

Get Write Access

Only users with permissions to the port get Write Access. The user with Write Access can send commands to the target device. Write Access can be transferred among users working in the HSC via the Get Write Access command.

To enable Write Access, choose Emulator > Click Get Write Access.

- You now have Write Access to the target device.
- When another user assumes Write Access from you:
 - The HSC displays a red block icon before Write Access in the status bar.
 - A message appears to the user who currently has Write Access, alerting that user that another user has taken over access to the console.

Get Write Lock

Write lock prevents other users from taking the write access while you are using it.

1. To get write lock, choose Emulator > Get Write Lock.
2. If Get Write Lock is not available, a request rejected message appears.

Write Unlock

To get Write Unlock, choose Emulator > Write Unlock.

Send Break

Some target systems such as Sun Solaris servers require the transmission of a null character (Break) to generate the OK prompt. This is equivalent to issuing a STOP-A from the Sun keyboard.

Only users with Write Access privileges can send a break.

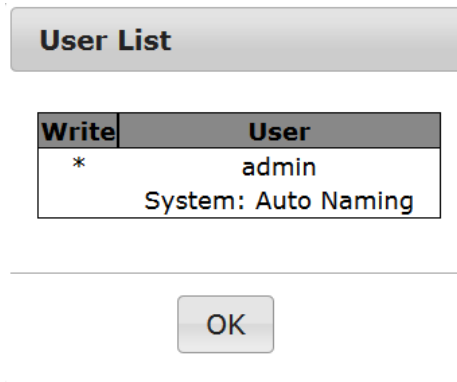
To send an intentional “break” to a Sun Solaris server:

1. Verify that you have Write Access. If not, follow the instructions in the previous section to obtain write access.
2. Choose Emulator > Send Break. A Send Break Ack (Acknowledgement) message appears.
3. Click OK.

Connected Users

The Connected Users command allows you to view a list of other users who are currently connected on the same port.

1. Choose Emulator > Connected Users.



2. A star appears in the Write column for the User who has Write Access to the console.

Exit

1. Choose Emulator > Exit to close the HSC.

Copy and Paste

Data on the current visible page can be selected for copying. Copy and Paste are accessible in the HSC by right click in the terminal window. Select Copy or Paste in the context menu that appears.

If you need to paste a large amount of data, it is better to save the data in a file and use the Send a Text File function. Pasting a large amount of data in a browser windows can cause the browser to hang as it processes the data. See *Send a Text File* (see "*Send Text File*" on page 356).

When pasting data to a port, the end of a line is sent as a carriage return.

The Cut option on the right-click menu is disabled.

Do not use the Delete option that appears in the right-click menu of IE and some versions of Firefox. This Delete option will remove display lines entirely from the emulator window.

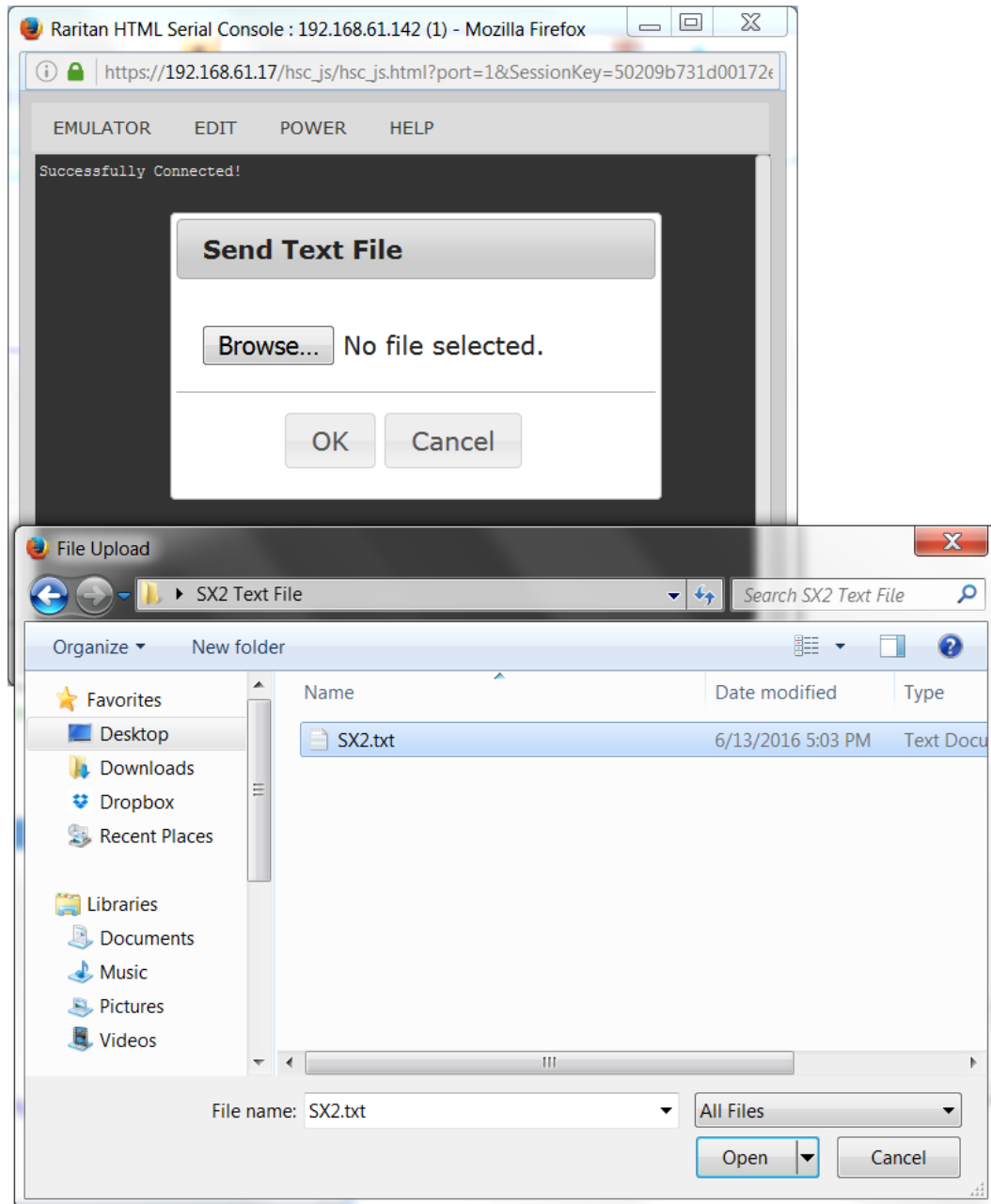
► Browser-specific behaviors

When copying from IE or Edge browsers, there are no end of line characters in the copied data. The pasted data appears to be all in one line and contains many spaces. When pasting back into a HSC window, the data may appear to be misaligned, but the data is complete.

Send Text File

1. Select Edit> Send Text File.
2. In the Send Text File dialog, click Browse to find the text file.
3. Click OK.
 - When you click OK, Raritan Serial Console (RSC) sends whatever file you selected directly to the port.

- If there is currently no target connected, nothing is visible on the screen.



► **Note, if you are using a Mac® and/or Safari®, do the following in order to use this feature:**

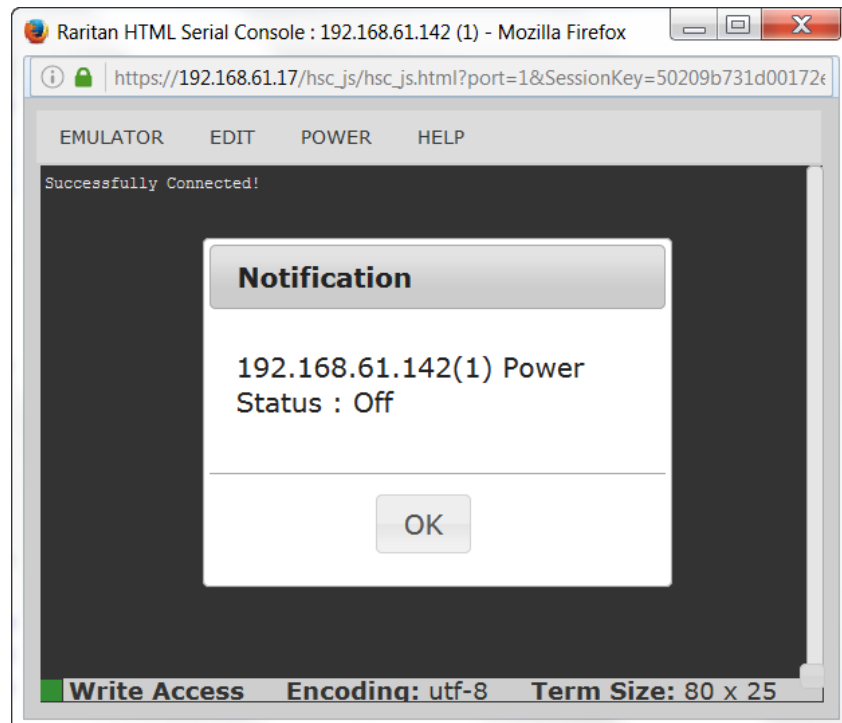
1. In Safari, select Preferences.
2. Under the Security tab, select "Manage Website Settings"

3. Click on the KX III website.
4. Select "Run in unsafe mode" from the drop-down box.
5. Restart Safari.

Power Status

Power Status in HSC shows the status of the outlet the target is plugged into.

1. Choose Power > Power Status.
2. The Notification dialog shows the status of the outlet as ON or OFF.



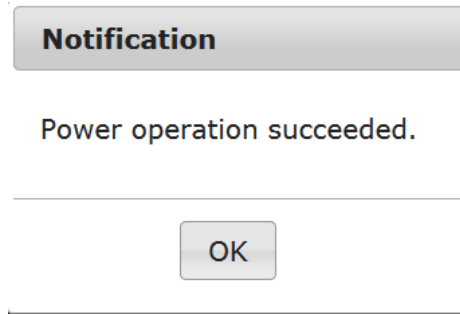
Power on a Target

Use this option to power on a target from HSC.

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

1. Select Power> Power On.

2. Click OK in the success message.

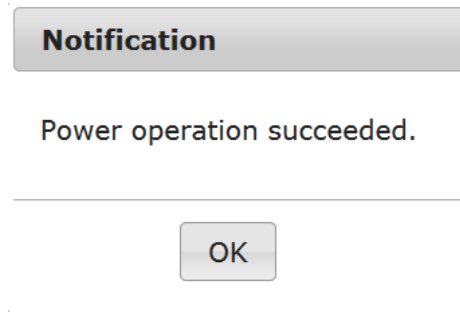


Power Off a Target

Use this option to power off a target from HSC.

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

1. Select Power> Power Off.
2. Click OK in the success message.



Power Cycle a Target

Power cycling allows you to turn a target off and then back on through the outlet it is plugged into.

This option is visible only when -

- there are one or more power associations to the target
- the target is already powered on (the port status is Up)
- you have permission to manage the target's power

1. Choose Power> Power Cycle.
2. Click OK in the success message.

Chapter 8 Dominion KX III User Station

To use a standalone appliance for remote access to KX III target servers instead of using the VKC or AKC clients on a PC or laptop, purchase Dominion User Stations from Raritan. The User Station is perfect for environments like labs, studios and control rooms where a PC or laptop is not wanted.

This chapter provides a brief introduction to the User Station. For detailed information, refer to the user documentation from the User Station's section on the Raritan website's *Support page* (<http://www.raritan.com/support/>).

In This Chapter

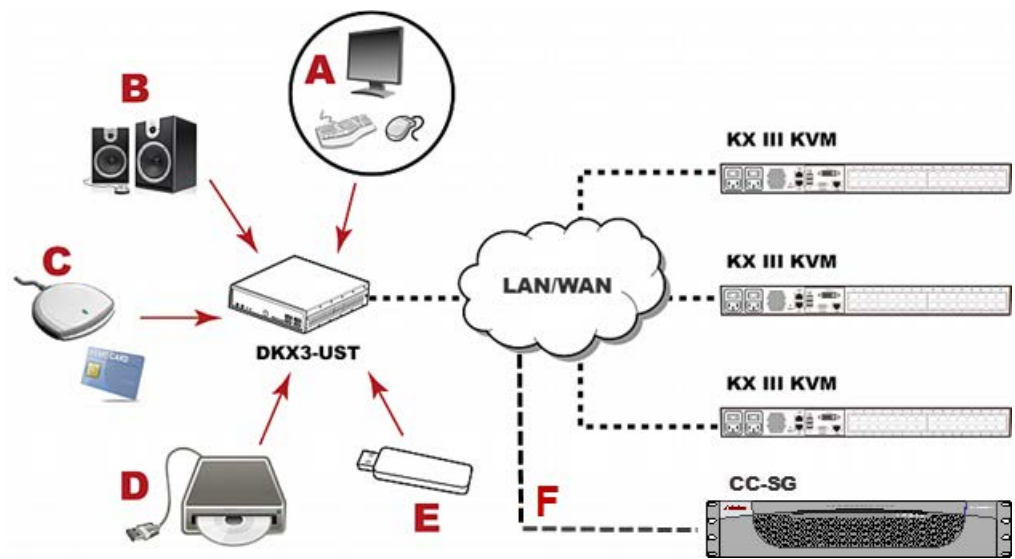
Overview	361
User Station Photo and Features	362
Operating the User Station	362

Overview

The Dominion User Station (DKX3-UST) is designed to access servers and computer devices connected to KX III's from your LAN/WAN networks. ALL KX III models are supported. KX III Release 3.2 and above is required.

One User Station can access the servers connected to multiple KX III's so that you can easily access a large number of servers with a single click.

Note that the User Station does NOT support the access to a target server which is from a tiered KX III or a blade server. Use VKC or AKC clients to access such targets instead.



A	A USB Keyboard, USB mouse, and one or two HDMI- or DisplayPort-interfaced monitors
B	Analog or digital audio appliances
C	Optional smart card reader for remote IT device authentication
D	External drives as virtual media, such as CD-ROM
E	USB drives for virtual media or User Station software update
F	Optional integration with CC-SG

User Station Photo and Features

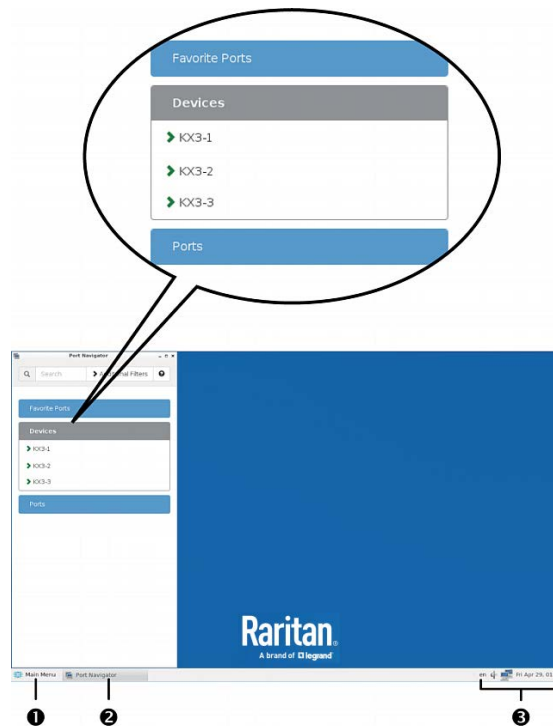


- Supports single or dual monitors
- Two 1080p streaming video sessions at 30 FPS
- Supports VGA, DVI, HDMI and DisplayPort video
- Favorites and hot-key switching
- Access hundreds of servers
- Ultra-fast connections and sub-second switching with the non-blocking DKX3-808 model
- Dual Gigabit Ethernet ports
- Self-contained, low maintenance appliance
- Desktop, rack and VESA mountable

Operating the User Station

1. Have the required equipment properly connected to the User Station.
 - a. Power OFF all devices.
 - b. Connect a USB keyboard, mouse and one or two monitors to the User Station.
 - c. Connect the User Station to the LAN/WAN network.
2. Power on and log in to the User Station.
 - For initial login, use Raritan's default username and password: **admin** and **raritan**.
3. Add KX III's data. See **Logging In to KX III** (on page 18).

4. The added KX III's are displayed in the Port Navigator window.



5. Click a KX III to show a list of its servers.
6. Click a target server, and a KVM Client opens, showing the target video. Now you can control the target with the attached keyboard and mouse.

For detailed information, refer to the user documentation from the User Station's section on the Raritan website's **Support page** (<http://www.raritan.com/support/>).

Chapter 9 Mobile KVM Client (MKC) Help

In This Chapter

Remotely Access Targets Using a Mobile Device	364
Connect to a Target Using the Mobile KVM Client	365
Touch Mouse Functions.....	365
Using the MKC Toolbar	366
Display Mobile Device Keyboard	368
Display Connection Info	368
Set Keyboard Type	369
Manage Mobile Client Keyboard Macros	369
Launch Keyboard Macro	370
Set Mouse Mode	370
Sync Mouse in Intelligent or Standard Mouse Mode.....	372
Auto-Sense Video Settings	372
Set Video Connection Quality.....	372
View MKC Help	373

Remotely Access Targets Using a Mobile Device

KX III supports remote access to targets from Apple® iPad® and iPhone® with IOS 4.0 (or later).

Mobile access is provided through Mobile Access Client, which requires the use of CommandCenter Secure Gateway (CC-SG).

Access and power control of your targets is supported using the Mobile KVM Client (MKC).

MKC launches automatically from mobile devices. There is no configuration or selection of MKC required. See ***Connect to a Target Using the Mobile KVM Client*** (on page 365)

You connect to each interface using the same links as when accessing from PC. When MKC opens, use the touch screen equivalent to each mouse click operation for navigating. See ***Touch Mouse Functions*** (on page 365).

The mobile device does not provide file storage for keyboard macros, so keyboard macros that you have created and would like to use in MKC can be stored on CC-SG with your profile data. You must import user-defined keyboard macros, using the desktop Access Client, before they will be available in MKC. See ***Manage Mobile Client Keyboard Macros*** (on page 369).

Connect to a Target Using the Mobile KVM Client

Mobile access using the Mobile Access Client requires the use of CommandCenter Secure Gateway (CC-SG).

Enable pop-ups in your mobile device browser before accessing Mobile KVM Client (MKC) or CC-SG Mobile Access Client.

MKC does not support connections over IPv6.

► To connect to a target via KX III on a mobile device:

1. Login to the Access Client using your mobile device browser.
2. Touch the node you want to access in the node list, then touch the blue interface link in the Node Profile to the right.
3. The Mobile KVM Client opens and connects to the target.

Touch Mouse Functions

Use the touchscreen equivalent for each mouse function to navigate the Mobile KVM Client (MKC) on your mobile device.

To view this chart in MKC, touch the Help icon (?) in the MKC toolbar.

Single Finger Touch	Mouse Equivalent
touch down - move - release	move mouse pointer
short tap	left click
double short tap	left double-click
short tap - touch down - move - release	hold down left mouse button and move, as in drag and drop or select
Two Finger Touch	Mouse Equivalent
touch down - move - release	move screen
touch down - change distance - release	resize screen (short pause at 100% zoom)
short tap	right click
double short tap	right double-click
short tap - touch down - move - release	hold down right mouse button and move, as in right drag and drop

Using the MKC Toolbar

The MKC toolbar may not be completely visible at one time, depending on the resolution of your mobile device.

▶ **To view the whole toolbar:**

- Touch and swipe to move the toolbar icons to the left and right, bringing different icons into view.

▶ **To use the keyboard button icons:**

The toolbar contains icons for each keyboard button you may need. Touch and swipe left and right to view all icons.

- Touch an icon for a button press.
- For a button hold, such as for Control and Alt used in Control+Alt+Delete, touch the icon once to activate it. The icon color will darken to indicate it is currently pressed. To release the icon, touch again.

MKC Toolbar Icons

Depending on your mobile device screen size and resolution, you may not see all toolbar icons at once. For example, on tablet device, such as an iPad you may see F4 as the final icon to the right.



Touch and swipe the toolbar to the left, to view the F5 through F12 icons. Swipe the toolbar back to the right to return to the default view.

On a mobile phone device, such as an iPhone, you will see fewer icons. Use the same touch-and-swipe motion left and right to view additional icons.

▶ Keyboard Icon

Provides access to the mobile device's native soft keyboard. See *Display Mobile Device Keyboard* (on page 368).

▶ Shift (SHIFT) - Control (CTRL) - Alternate (ALT)

Provide the modifier keys to be used together with other keys on the toolbar. See *Using the MKC Toolbar* (on page 366).

▶ Windows (WIN)

Provides access to the Windows Start menu. This is the equivalent of the Windows key on a standard Windows keyboard.

▶ Application Key or "Right-Click" Key

Provides access to a right-click menu. This is the equivalent of the Application key on a standard Windows keyboard. The Application key has an image of a mouse pointer on a menu, and it is positioned between the Alt and Ctrl keys to the right of the spacebar.

Touch the Application icon to display the selected item's right-click menu.

▶ Left Arrow, Up Arrow, Down Arrow, Right Arrow

Provide document navigation.

▶ Tab (TAB) - Escape (ESC) - Delete (DEL) - Function 1 (F1) thru Function 12 (F12)

Provide standard press and release key operation.

Display Mobile Device Keyboard

Toggle on and off the MKC keyboard to display or hide it.

The keyboard is configured on the mobile device. For example, on iPad choose Settings > General > Keyboard > International Keyboards to see the available keyboards or to add a keyboard. From the soft keyboard touch the globe icon to toggle between available keyboards.

▶ To display/hide mobile device keyboard:

- In the MKC toolbar, touch the keyboard icon, next to the Menu button to display the keyboard.
- In the keyboard, touch the icon in the bottom right corner to hide the keyboard.

Display Connection Info

Display information about your connection to see how much bandwidth is being used in transmitting and receiving data.

This information can be helpful in determining how much of the available bandwidth is being consumed, the effect of selecting a lower video quality setting, or for troubleshooting if image updates are slower than expected. See *Set Video Connection Quality* (on page 372).

Incoming	kpx/s	pixel updates per second
	kB/s	bytes per second
Outgoing	msg/s	messages per second
	kB/s	bytes per second

▶ To display connection info:

- In the MKC toolbar, touch Menu, then touch Connection Info.

The connection information appears in the viewer.

To turn off the connection information display, touch Menu, then touch Connection Info. The display toggles off.

Set Keyboard Type

The default keyboard in MKC is US/International English. Select the language keyboard to match the language keyboard setting of the target you are accessing. This is required to provide the correct keyboard mapping in the target.

You must correctly set the keyboard type in MKC based on the language mapping required by the target. This setting is in addition to the keyboard language setting on your mobile device itself.

▶ To set keyboard type:

1. In the MKC toolbar, touch Menu, then touch Keyboard Type.
2. Touch the keyboard language to set it.

Keyboard Languages

- Danish (Denmark)
- English (UK)
- English (US/Int'l)
- French (Belgium)
- French (France)
- German (Germany)
- German (Switzerland)
- Hungarian
- Italian (Italy)
- Japanese
- Korean (Korea)
- Norwegian (Norway)
- Portuguese (Portugal)
- Slovenian
- Spanish (Spain)
- Swedish (Sweden)

Manage Mobile Client Keyboard Macros

Each user must import their user-defined keyboard macros to make them available for use while connected to targets using the Mobile KVM Client (MKC).

Export the file from Virtual KVM Client (VKC), then import it using the desktop Access Client. You cannot import macros using a mobile device. Imported macros are available per user in MKC when you connect to a target using your mobile device.

Launch Keyboard Macro

Pre-defined macros are always available in MKC. You must import user-defined macros using the desktop Access Client before they are available on MKC. See *Manage Mobile Client Keyboard Macros* (on page 369).

SUN macros are available in MKC if you are connected to a target that has the SUN CIM.

► To launch keyboard macro:

1. In the MKC toolbar, touch Menu, then touch Keyboard Macros.
2. Touch the macro you want to launch.

The macro is launched and the results display on the target.

Set Mouse Mode

When controlling a target server, the MKC displays two mouse cursors: a red bullseye indicates where the mobile touch gestures are relative to the target, and the cursor that belongs to the target server.

Single mouse mode is not available in MKC.

Your mouse will operate in dual mouse mode only. When properly configured, the two mouse cursors align.

There are several mouse modes when in dual mouse mode. Mouse modes are available based on the attached CIM and selected USB profile.

- See *Absolute Mouse Mode* (on page 371).
- See *Intelligent Mouse Mode* (on page 371).
- See *Standard Mouse Mode* (on page 371).

► To set mouse mode:

1. In the MKC toolbar, touch Menu, then touch Mouse.
2. Touch Mouse Mode, then touch Absolute, Intelligent, or Standard.

Absolute Mouse Mode

In this mode, absolute coordinates are used to keep the client and target cursors in synch, even when the target mouse is set to a different acceleration or speed.

This mode is supported on servers with USB ports and is the default mode for virtual media CIMs.

Absolute Mouse Synchronization requires the use of a virtual media CIM -

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

D2CIM-DVUSB-DP

Note: For KX II, Absolute Mouse Synchronization is available for use with the virtual media-enabled USB CIM (D2CIM-VUSB and D2CIM-DVUSB) only.

Intelligent Mouse Mode

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target. Intelligent mouse mode is the default for non-VM targets.

During synchronization, the mouse cursor does a “dance” in the top left corner of the screen and calculates the acceleration. For this mode to work properly, certain conditions must be met.

See the Dominion KXII User Guide for more details on Intelligent Mouse mode.

Standard Mouse Mode

Standard Mouse mode uses a standard mouse synchronization algorithm. The algorithm determines relative mouse positions on the client and target server.

In order for the client and target mouse cursors to stay in synch, mouse acceleration must be disabled. Additionally, specific mouse parameters must be set correctly.

Sync Mouse in Intelligent or Standard Mouse Mode

In Intelligent or Standard mouse mode, the Sync Mouse command forces realignment of the target server mouse pointer with the MKC mouse pointer.

► **To sync mouse:**

1. In the MKC toolbar, touch Menu, then touch Mouse.
2. Touch Sync Mouse. Wait several seconds while the synchronization occurs.

Auto-Sense Video Settings

The Auto-sense Video Settings command forces a re-sensing of the video settings (resolution, refresh rate) and redraws the video screen.

Auto-sensing video settings can eliminate target video misalignment and sometimes mouse synchronization problems.

► **To auto-sense video settings:**

1. In the MKC toolbar, touch Menu, then touch Video.
2. Touch Auto Sense Video Settings.

Set Video Connection Quality

Adjust the bandwidth consumed by the connection by setting the video connection quality. A lower quality setting will consume less bandwidth by providing lower video quality.

Use the connection information display to get bandwidth information to help adjust the video connection quality. See *Display Connection Info* (on page 368).

► **To set video connection quality:**

1. In the MKC toolbar, touch Menu, then touch Video.
2. Touch Connection Quality Settings, then touch High, Medium, or Low. The default setting is High.

View MKC Help

Descriptions of the touchscreen techniques can be accessed in MKC.

▶ To view MKC help:

- Touch the Help icon (?) icon in the toolbar. The help opens.
- See ***Touch Mouse Functions*** (on page 365) to view this information.

Chapter 10 KX III Remote Console

In This Chapter

Overview	374
Scanning Ports - Remote Console	375
Changing a Password	380
Managing Favorites.....	381

Overview

When you log in to the KX III via a network connection, you access the Remote Console. The first page accessed is the Port Access page.

See *Logging In to the KX III* (see "Logging In to KX III" on page 18) and *Port Access Page (Remote Console Display)* (on page 21)



Dominion® KX III

Time & Session:
January 23, 2018 19:02:02

User: admin
State: 60 min idle
Your IP: 192.168.32.61
Last Login: Jan 15, 2018 11:57:08

Device Information:
Device Name: kx3-61-16
IP Address:
192.168.61.16
192.168.60.53
f007.2fa.6c4f.2032.20d.5aff.te00.25f
f007.2fa.6c4f.2031.20d.5aff.te00.260
Firmware: 3.5.0.5.1802
Device Model: DIOK3-132
Network: LAN1 LAN2
PowerIn1: on
PowerIn2: off

Port States:
2 Ports: up
30 Ports: down
32 Ports: idle

Connected Users:
admin (192.168.32.61)
60 min idle

Online Help

Port Access |
 Power |
 Virtual Media |
 User Management |
 Device Settings |
 Security |
 Maintenance |
 Diagnosics |
 Help

[Home](#) > [Ports](#)

Port Access

*Click on the individual port name to see allowable operations.
0 / 1 Remote KVM channels currently in use.*

View By Port	View By Group	View By Search	Set Scan			
▲ No.	Name	Type	Status	Availability		
1	Target 9-RSAIL-SLIMLINE	Dual-VM	up	idle		
2	SYSMETEST-OPTIPELEX	Dual-VM	up	idle		
3	Dominion_KX3_Port3	Not Available	down	idle		
4	Dominion_KX3_Port4	Not Available	down	idle		
5	Dominion_KX3_Port5	Not Available	down	idle		
6	Dominion_KX3_Port6	Not Available	down	idle		
7	Dominion_KX3_Port7	Not Available	down	idle		
8	Dominion_KX3_Port8	Not Available	down	idle		
9	Dominion_KX3_Port9	Not Available	down	idle		
10	Dominion_KX3_Port10	Not Available	down	idle		
11	Dominion_KX3_Port11	Not Available	down	idle		
12	Dominion_KX3_Port12	Not Available	down	idle		
13	Dominion_KX3_Port13	Not Available	down	idle		
14	Dominion_KX3_Port14	Not Available	down	idle		
15	Dominion_KX3_Port15	Not Available	down	idle		
16	Dominion_KX3_Port16	Not Available	down	idle		
17	Dominion_KX3_Port17	Not Available	down	idle		

Use the Remote Console to access and scan target servers, manage favorites, and change your password.

For more in the Remote Console interface elements, see *KX III Remote Console Interface* (on page 20).

Scanning Ports - Remote Console

Use the port scanning feature to search for selected targets and display them in individual thumbnails as part of a slide show.

This feature allows you to monitor up to 32 targets at one time since you can view each target server individually as it is displayed during the slide show.

Connect to targets or focus on a specific target as needed.

Scans can include standard targets, blade servers, tiered Dominion devices, and KVM switch ports.

For dual video port groups, the primary port is included in a port scan, but the secondary port is not included when connecting from a remote client. Both ports can be included in the scan from the Local Port.

Note: The scan port feature is available from the Remote Console and Local Console, but the feature varies slightly.

Scanning Ports Slide Show - Remote Console

When you start a scan, the Port Scan window opens.

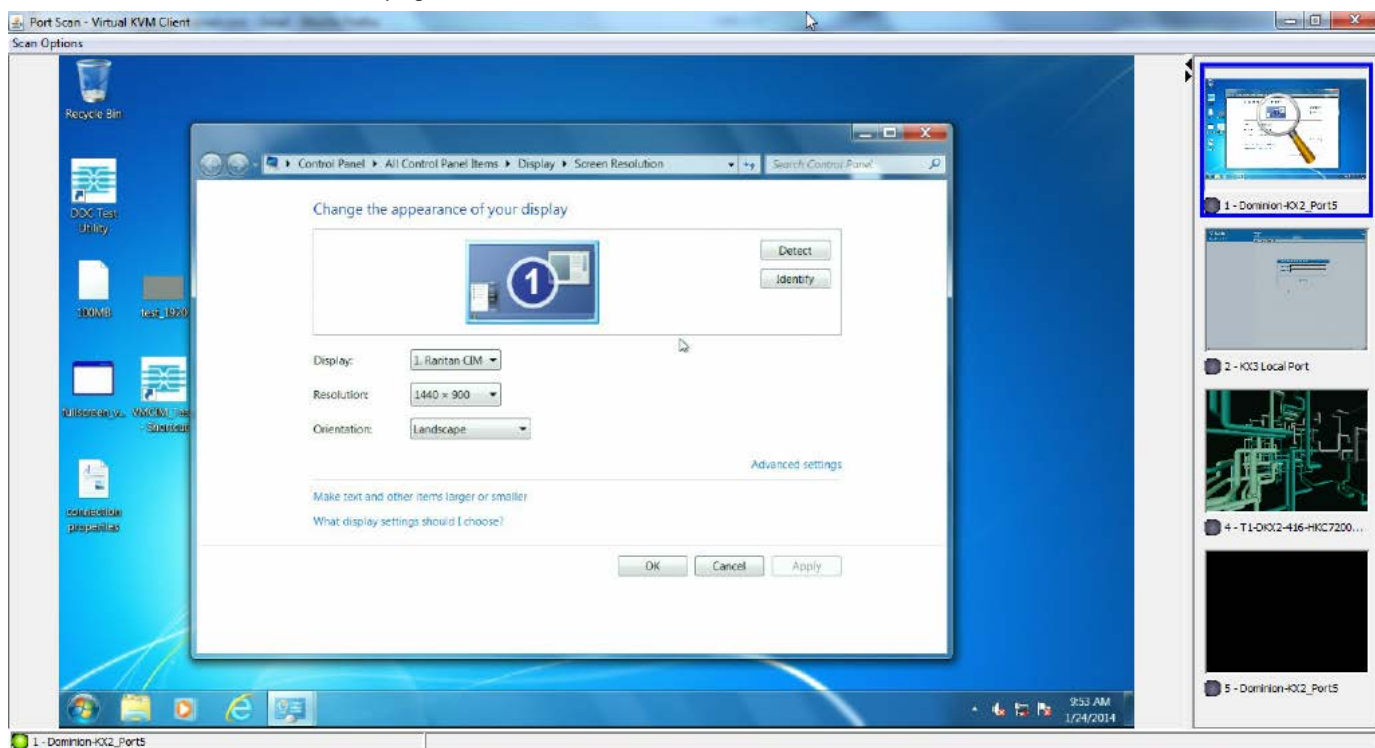
As each target is found, it is displayed as a thumbnail in a slide show.

The slide show scrolls through the target thumbnails based on the default interval of 10 seconds or according to the interval you specify.

As the scan scrolls through the targets, the target that is the focus of the slide show displays in the center of the page.

The name of the target is displayed below its thumbnail and in the task bar at the bottom of the window.

If a target is busy, a blank screen is displayed instead of the target server access page.



Configure scan settings for the Remote Console from VKC, VKCS, or AKC.

See *Configuring Port Scan Settings in VKC/VKCS and AKC* (on page 283)

Note: Scan port settings for the Local Console are configured on the Local Port Settings page. See Scanning Ports - Local Console (on page 389)

Target Status Indicators During Port Scanning - Remote Console

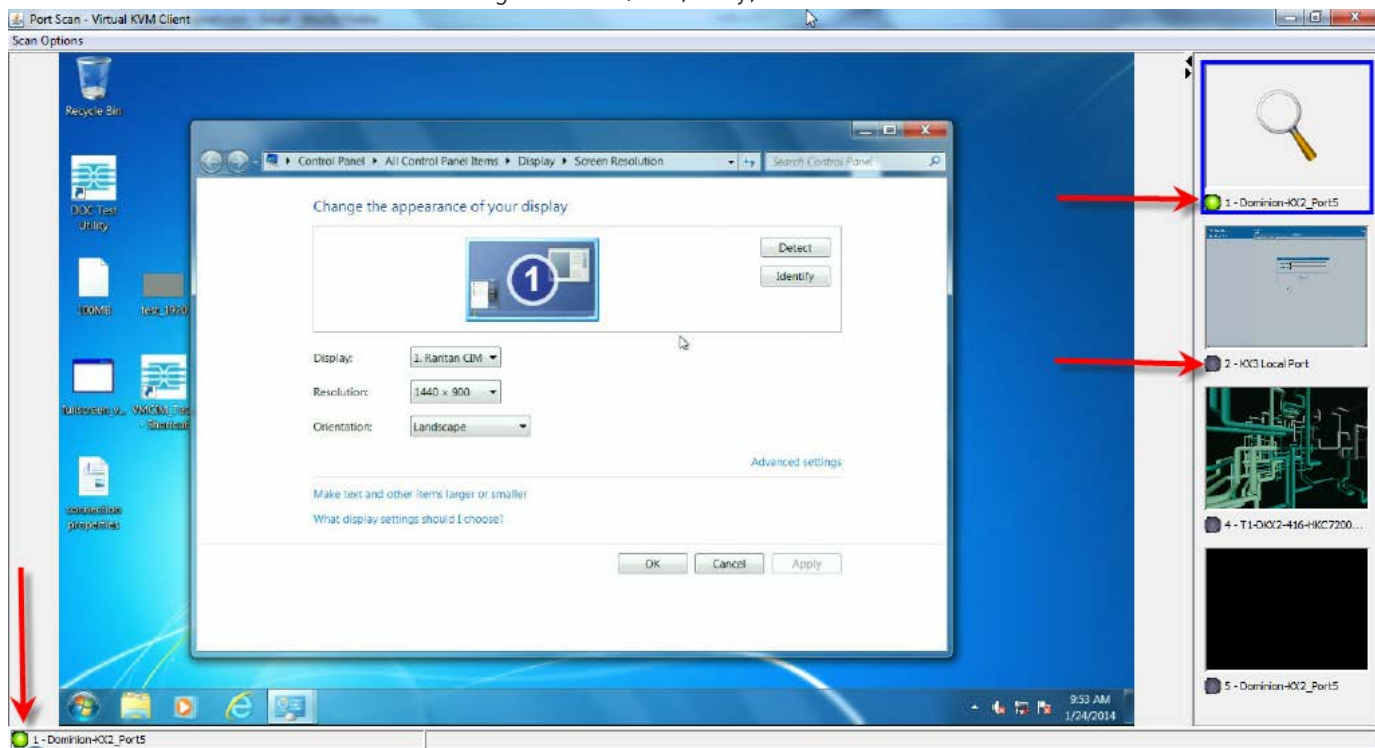
The status of each target is indicated by green, yellow and red lights that are displayed below the target thumbnail.

As the target is the focus of the rotation, the indicator is in the task bar also shows the status.

Lights for each target are gray until they are the focus of the slide show.

The status lights indicate the following:

- Green - the target is up/idle or up/connected
- Yellow - the target is down but connected
- Red - the target is down/idle, busy, or otherwise not accessible



Using Scan Port Options

Following are options available to you while scanning targets.

With the exception of the Expand/Collapse icon, all of these options are selected from the Options menu in the upper left of the Port Scan viewer.

The options will return to their defaults when you close the window.

*Note: Configure scan settings such as the display interval from either the Virtual KVM Client (VKC) or Active KVM Client (AKC). See **Configuring Port Scan Settings in VKC/VKCS and AKC** (on page 283)*

► Hide or View Thumbnails

- Use the Expand/Collapse icon  at the upper left of the window to hide or view thumbnails. Expanded is the default view.

► Pause the Thumbnail Slide Show

- Pause thumbnails from rotating between one target and the next by selecting Options > Pause. Rotating thumbnails is the default setting.

► Resume the Thumbnail Slide Show

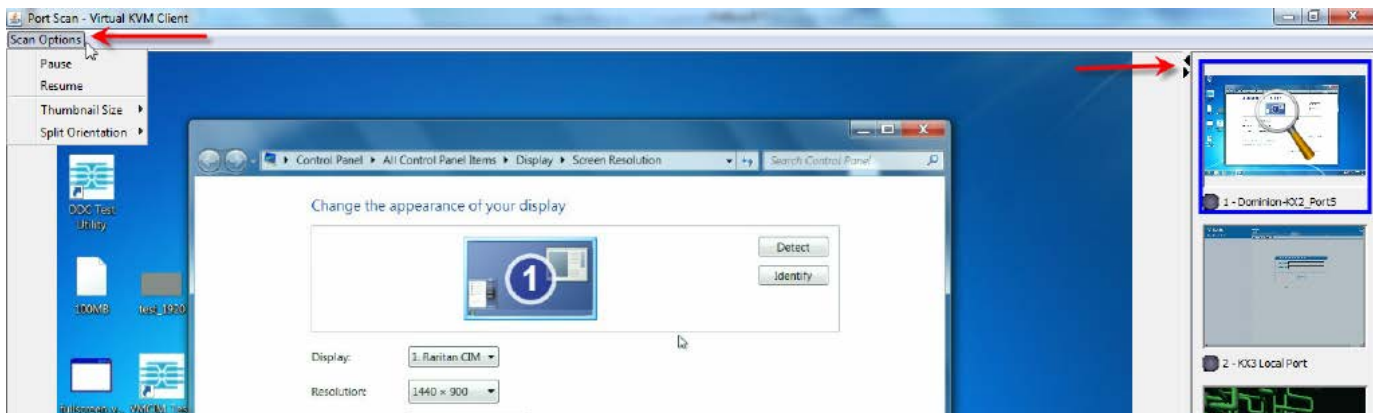
- Resume the thumbnail rotation by selecting Options > Resume.

► Size the Thumbnails in the Port Scan Viewer

- Enlarge the size of the thumbnails by selecting Options > Size > 360x240.
- Minimize the size of the thumbnails by selection Options > Size > 160x120. This is the default thumbnail size.

► Change the Orientation of the Port Scan Viewer

- View thumbnails along the bottom of the Port Scan viewer by selecting Options > Split Orientation > Horizontal.
- View thumbnails along the right of the Port Scan viewer by selecting Options > Split Orientation > Vertical. This is the default view.

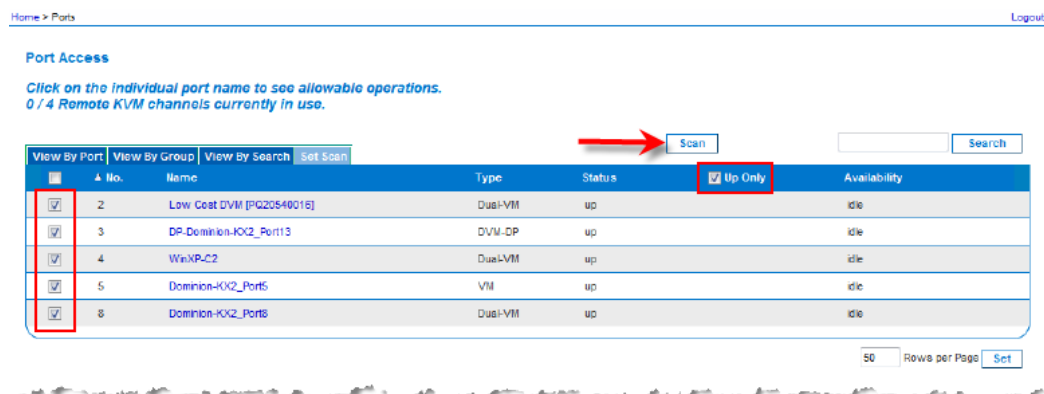


Scan for Targets

► To scan for targets:

1. Click the Set Scan tab on the Port Access page.
2. Select the targets you want to include in the scan by selecting the checkbox to the left of each target, or select the checkbox at the top of the target column to select all targets.
3. Leave the Up Only checkbox selected if you only want targets that are up to be included in the scan. Deselect this checkbox if you want to include all targets, whether up or down.
4. Click Scan to begin the scan.

As each target is scanned, it is displayed in slide show view on the page.



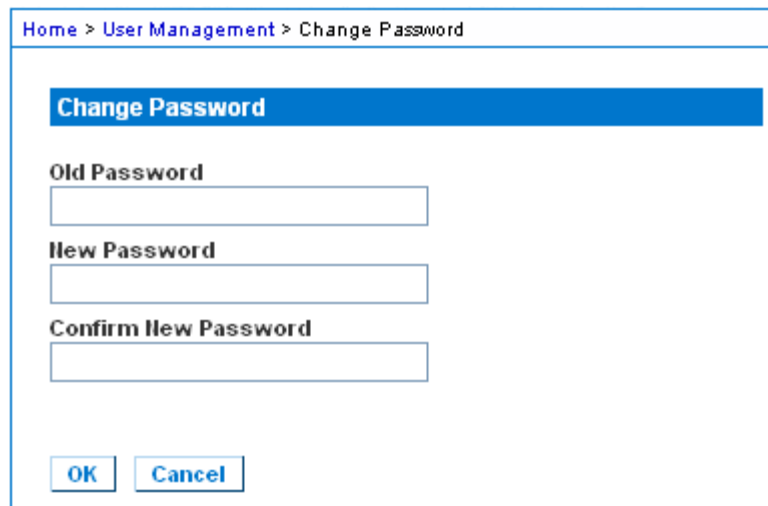
5. Click Options > Pause to pause the slide show and stop it from moving between targets, click Options > Resume to resume the slide show.
6. Click on a target thumbnail to scan it next.
7. Connect to a target by double clicking on its thumbnail.

Changing a Password

► **To change your KX III password:**

1. Choose User Management > Change Password. The Change Password page opens.
2. Type your current password in the Old Password field.
3. Type a new password in the New Password field. Retype the new password in the Confirm New Password field. Passwords can be up to 64 characters in length and can consist of English alphanumeric characters and special characters.
4. Click OK.
5. You will receive confirmation that the password was successfully changed. Click OK.

*Note: If strong passwords are in use, this page displays information about the format required for the passwords. For more information about passwords and strong passwords, see **Strong Passwords** (on page 190) in online help.*



The screenshot shows a web browser window with the address bar displaying 'Home > User Management > Change Password'. The main content area has a blue header bar with the text 'Change Password'. Below this, there are three text input fields labeled 'Old Password', 'New Password', and 'Confirm New Password'. At the bottom of the form, there are two buttons: 'OK' and 'Cancel'.

Managing Favorites

A Favorites feature is provided so you can organize and quickly access the devices you use frequently.

The Favorite Devices section is located in the lower left sidebar of the Port Access page and provides the ability to:

- Create and manage a list of favorite devices
- Quickly access frequently-used devices
- List your favorites either by Device Name, IP Address, or DNS hostname
- Discover KX III devices on its subnet
- Retrieve discovered KX III devices from the connected Dominion device

Enable Favorites

- Click Enable in the Favorite Devices section of the left panel of the KX III interface.



Access and Display Favorites

► **To access a favorite KX III devices:**

- Click on a KX III listed beneath Favorite Devices in the left of the Remote Console.

► **To display favorite KX IIIs by name:**

- Click Display by Name.

► **To display favorite KX IIIs by IP Address:**

- Click Display by IP.

► **To display favorite KX IIIs by the host name:**

- Click Display by Host Name.



Discovering Devices on the Local Subnet

This option discovers KX III devices on your local subnet. This is the subnet where the KX III Remote Console is running.

These devices can be accessed directly from this page or you can add them to your list of favorites.

► **To discover devices on the local subnet:**

1. Choose Manage > Discover Devices - Local Subnet. The Discover Devices - Local Subnet page appears.
2. Choose the appropriate discovery port:
 - To use the default discovery port, select the Use Default Port 5000 checkbox.
 - To use a different discovery port:
 - a. Deselect the Use Default Port 5000 checkbox.
 - b. Type the port number in the Discover on Port field.
 - c. Click Save.

3. Click Refresh. The list of devices on the local subnet is refreshed.

► **To add devices to your Favorites List:**

1. Select the checkbox next to the device name/IP address.
2. Click Add.

► **To access a discovered device:**

- Click the device name or IP address for that device. A new browser opens to that device.

Discovering Devices on the KX III Subnet

This feature is only available in the Java client , RSC.

This option discovers KX III devices on the device subnet. This is the subnet of the KX III device's IP address.

You can access these devices directly from the Subnet page or add them to your list of favorites.

This feature allows multiple KX III devices to interoperate and scale automatically.

The KX III Remote Console automatically discovers the KX III devices, and any other Raritan device, in the subnet of the KX III.

► **To discover devices on the device subnet:**

1. Choose Manage > Discover Devices - KX III Subnet.



The Discover Devices - KX III Subnet page appears.

2. Click Refresh. The list of devices on the local subnet is refreshed.

► **To add devices to your Favorites List:**

1. Select the checkbox next to the device name/IP address.
2. Click Add.

► **To access a discovered device:**

- Click the device name or IP address for that device. A new browser opens to that device.

Chapter 11 KX III Local Console

In This Chapter

Overview	385
Accessing a Target Server	385
Local Console Video Resolution Behavior	386
Simultaneous Users.....	386
Local Port Hot Keys and Connect Keys.....	386
Scanning Ports - Local Console	389
Local Console Smart Card Access	394
Local Console USB Profile Options.....	395
KX III Local Console Factory Reset	396
Resetting the KX III Using the Reset Button on the Device	397

Overview

The Local Console interface provides access to the KX III while at the rack.

This section contains help on tasks performed by end users at the Local Console.

Accessing a Target Server

- ▶ **To access a target server:**
 1. Click the Port Name of the target you want to access. The Port Action Menu is displayed.
 2. Choose Connect from the Port Action menu. The video display switches to the target server interface.

Local Console Video Resolution Behavior

By default, monitors are typically set to the highest resolution they support.

Once a monitor is connected to the KX III Local Console, KX III detects the monitor's native resolution. As long as the native resolution is supported by the Local Console, KX III uses that resolution.

If the native resolution is not supported by the Local Console, and no other resolution is supported by the monitor and Local Console, KX III uses the resolution of the last monitor that was connected to the Local Console.

For example, you connect a monitor set to a resolution of 1600x1200@60Hz to the KX III Local Console. KX III uses that resolution since it is supported by the Local Console.

If the next monitor you connect to the Local Console is not set to a supported resolution, KX III uses the resolution of 1024x768@60.

For a list of supported Local Console video resolutions, see ***Supported KX III Local Port DVI Resolutions*** (see "***KX III Supported Local Port DVI Resolutions***" on page 420).

Consider reviewing ***Video Mode and Resolution Notes*** (on page 454) for additional information.

Simultaneous Users

The KX III Local Console provides an independent access path to the connected KVM target servers.

Using the Local Console does not prevent other users from simultaneously connecting over the network. And even when remote users are connected to the KX III, you can still simultaneously access your servers from the rack via the Local Console.

Local Port Hot Keys and Connect Keys

Because the KX III Local Console interface is completely replaced by the interface for the target device you are accessing, a hot key is used to disconnect from a target and return to the local port GUI.

A connect key is used to connect to a target or switch between targets.

The Local Port hot key allows you to rapidly access the KX III Local Console user interface when a target device is currently being viewed.

See ***Select the Local Port Hotkey*** (on page 141) and ***Select the Local Port Connect Key*** (on page 142) for more information.

Return to the Local Console from a Target Device - Default Hot Key

- Press the Scroll Lock hot key twice rapidly
The video display switches from the target device interface to the KX III Local Console interface.

Local Port Auto-Sense (Video Refresh) - Default Hot Key

► **To perform an auto-sense (video refresh) on the KX III local port via hot key:**

- Press and hold the Shift key, and quickly press the Scroll Lock key twice, and then release.

Connect Key Examples**Standard servers**

Connect key action	Key sequence example
Access a port from the local port	• Press Left ALT > Press and Release 5 > Release Left ALT
Switch between ports	• Press Left ALT > Press and Release 1 > Press and Release 1 > Release Left ALT
Disconnect from a target and return to the local port	• Double-click Scroll Lock

Blade chassis

Connect key action	Key sequence example
Access a port from the local port GUI	Access port 5, slot 2: • Press Left ALT > Press and Release 5 > Press and Release - > Press and Release 2 > Release Left ALT
Switch between ports	Switch from target port 5, slot 2 to port 5, slot 11: • Press Left ALT > Press and Release 5 > Press and Release - > Press and Release 1 > Press and Release 1 > Release Left ALT
Disconnect from a target and return to	Disconnect from target port 5, slot 11 and return to the local port GUI (the page from

the local port GUI	which you connected to target): • Double Click Scroll Lock

Special Sun Key Combinations

The following key combinations for Sun™ Microsystems server's special keys operate on the Local Console port. These special keys are available from the Keyboard menu when you connect to a Sun target device:

Sun key	Local port key combination
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
Mute	Ctrl + Alt + F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	No key combination
Power	No key combination

Scanning Ports - Local Console

Use the port scanning feature to search for selected targets and display them in individual thumbnails as part of a slide show.

This feature allows you to monitor up to 32 targets at one time since you can view each target server individually as it is displayed during the slide show.

Connect to targets or focus on a specific target as needed.

Scans can include standard targets, blade servers, tiered Dominion devices, and KVM switch ports.

For dual video port groups, the primary port is included in a port scan, but the secondary port is not included when connecting from a remote client. Both ports can be included in the scan from the Local Port.

Click on the thumbnail of any target server to exit scan mode and connect to the target, or use the Local Port ConnectKey sequence.

To exit scan mode, click the Stop Scan button in the thumbnail view, or use the DisconnectKey sequence hot key.

*Note: The scan port feature is available from the Remote Console and Local Console, but the feature varies slightly. See **Scanning Ports - Remote Console** (on page 375)*

Scanning Port Slide Show - Local Console

When you start a scan, the Port Scan window opens.

As each target is found, it is displayed as a thumbnail in a slide show.

The slide show scrolls through the target thumbnails based on the default interval of 10 seconds or according to the interval you specify.

As the scan scrolls through the targets, the target that is the focus of the slide show displays in the center of the page.

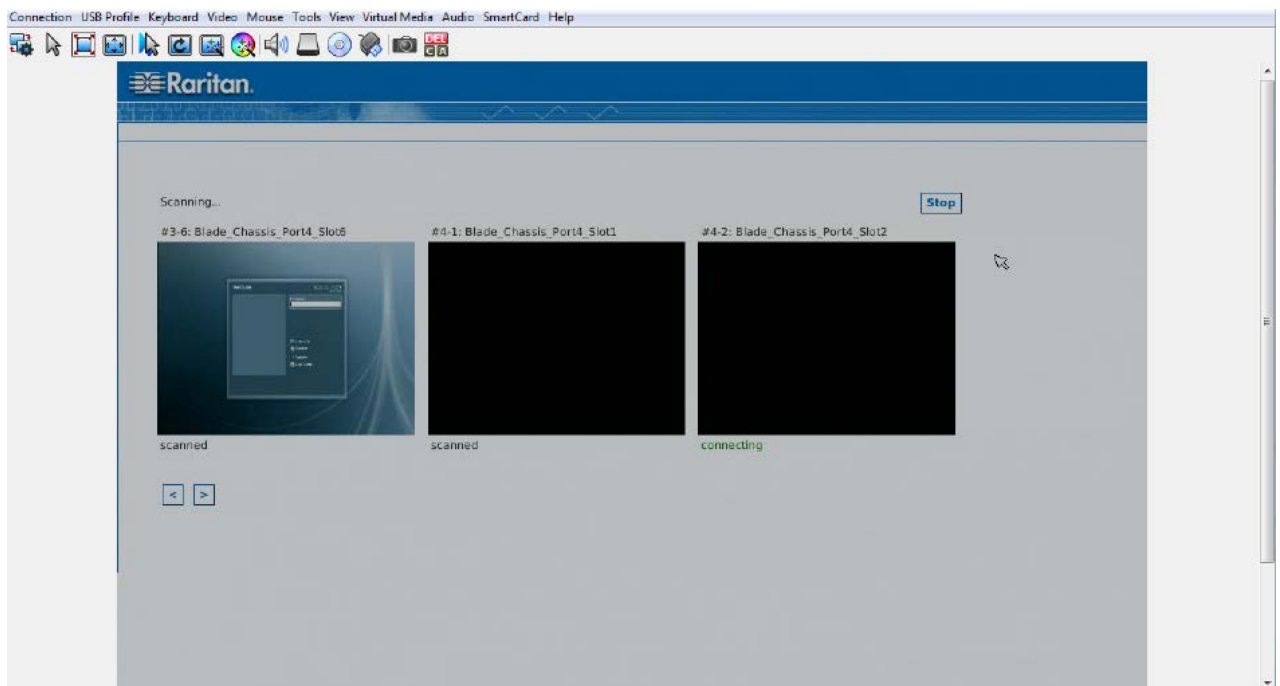
The name of the target is displayed below its thumbnail and in the task bar at the bottom of the window.

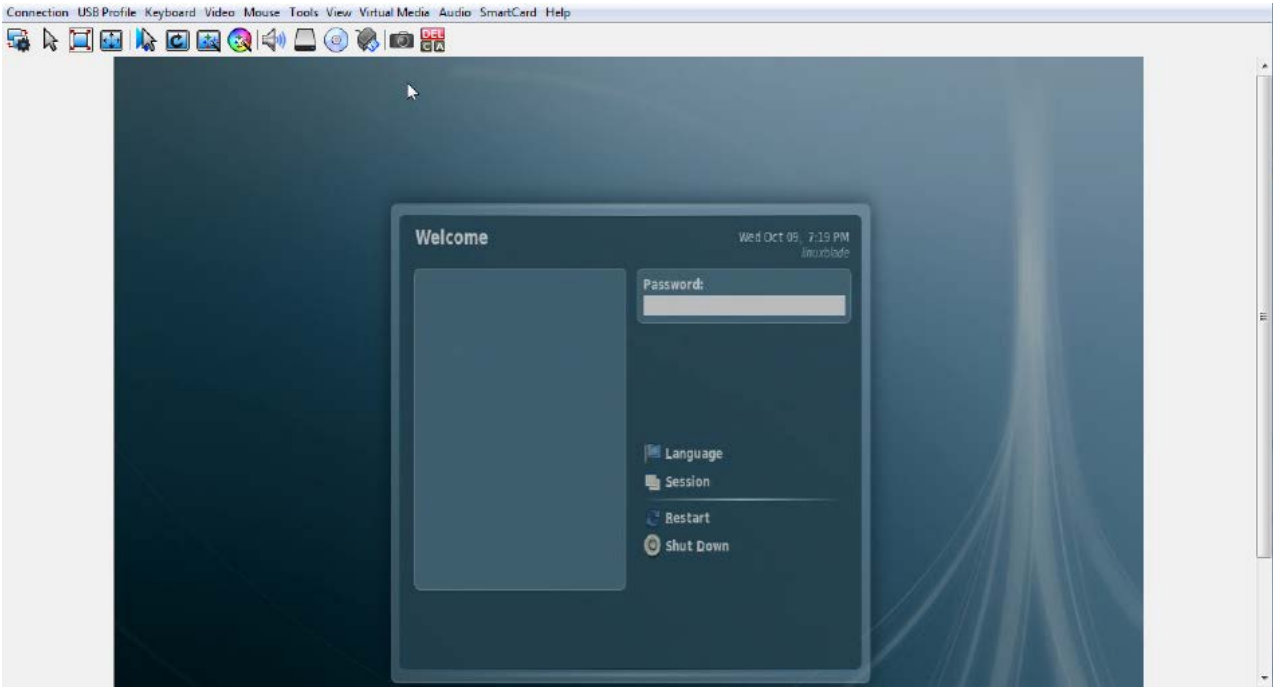
If a target is busy, a blank screen is displayed instead of the target server access page.

Configure the time between the slide show thumbnail rotation and the thumbnail focus interval on the Local Port Settings page.

See ***Configure Local Console Scan Settings*** (on page 392)

*Note: Configure scan settings for the Remote Console from VKC, VKCS, or AKC. See **Configuring Port Scan Settings in VKC/VKCS and AKC** (on page 283)*



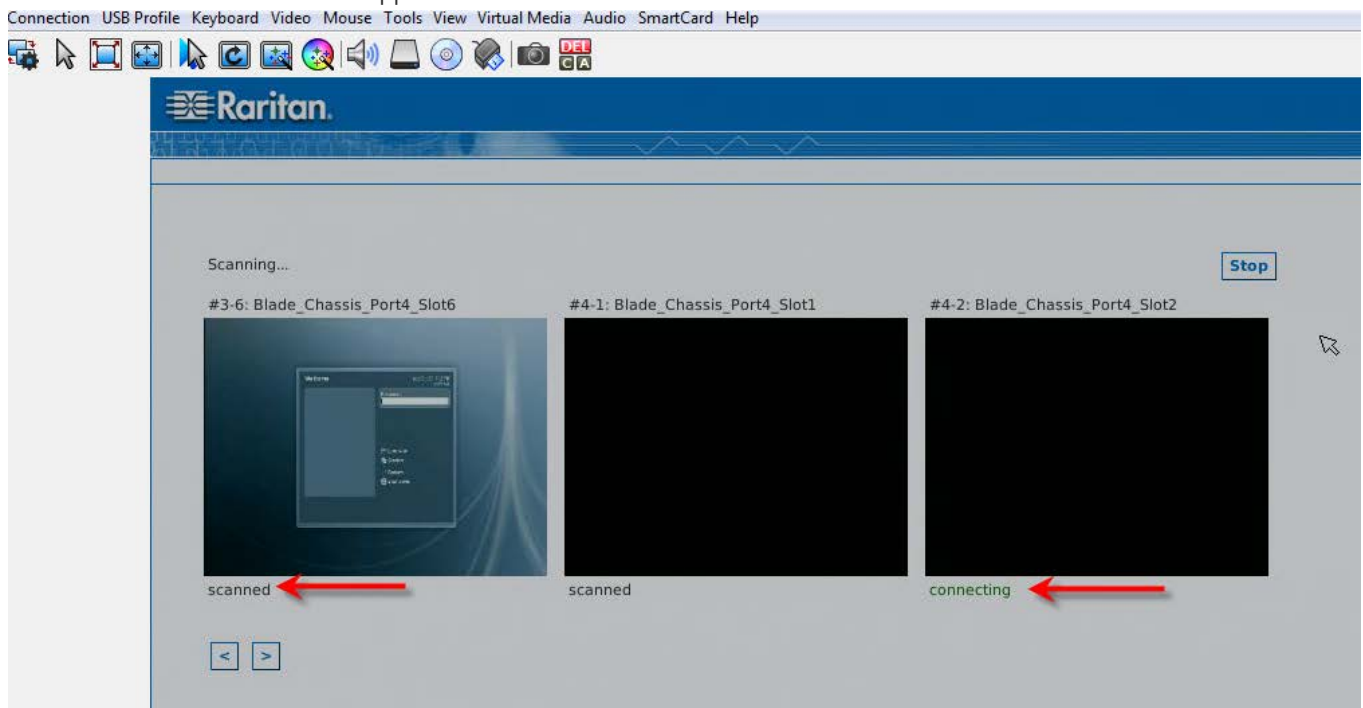


Target Status Indicators During Port Scanning - Local Console

In thumbnail view on the Local Console, the status of each target is indicated below the thumbnail on the page until it is the focus of the slide show view.

The scanning status of each target is displayed as:

- not scanned
- connecting
- scanned
- skipped



Configure Local Console Scan Settings

Do the following to configure Local Console scan port options.

*Note: Configure scan settings for the Remote Console from VKC, VKCS, or AKC. See **Configuring Port Scan Settings in VKC/VKCS and AKC** (on page 283)*

► **To configure the Local Console scan port settings:**

1. On the Local Console, select Device Settings.
2. In the Local Port Settings section, select Local Port Scan Mode.
3. Change the display interval as needed:

- Display Interval - changes the scan display interval.
- Interval Between Ports - change interval between switching different port during scan.

Scan for Targets - Local Console

► **To scan for targets:**

1. Click the Set Scan tab on the Port Access page.
2. Select the targets you want to include in the scan by selecting the checkbox to the left of each target, or select the checkbox at the top of the target column to select all targets.
3. Leave the Up Only checkbox selected if you only want targets that are up to be included in the scan. Deselect this checkbox if you want to include all targets, whether up or down.
4. Click Scan to begin the scan.

As each target is scanned, it is displayed in slide show view on the page.

Local Console Smart Card Access

To use a smart card to access a server at the Local Console, plug a USB smart card reader into the KX III using one of the USB ports located on the KX III.

Once a smart card reader is plugged in or unplugged from the KX III, the KX III autodetects it.

For a list of supported smart cards and additional system requirements, see ***Supported Smart Card Readers*** (on page 430), ***Unsupported Smart Card Readers*** (on page 431) and ***Smart Card Minimum System Requirements*** (on page 429).

When mounted onto the target server, the card reader and smart card will cause the server to behave as if they had been directly attached.

Removal of the smart card or smart card reader will cause the user session to be locked or you will be logged out depending on how the card removal policy has been setup on the target server OS.

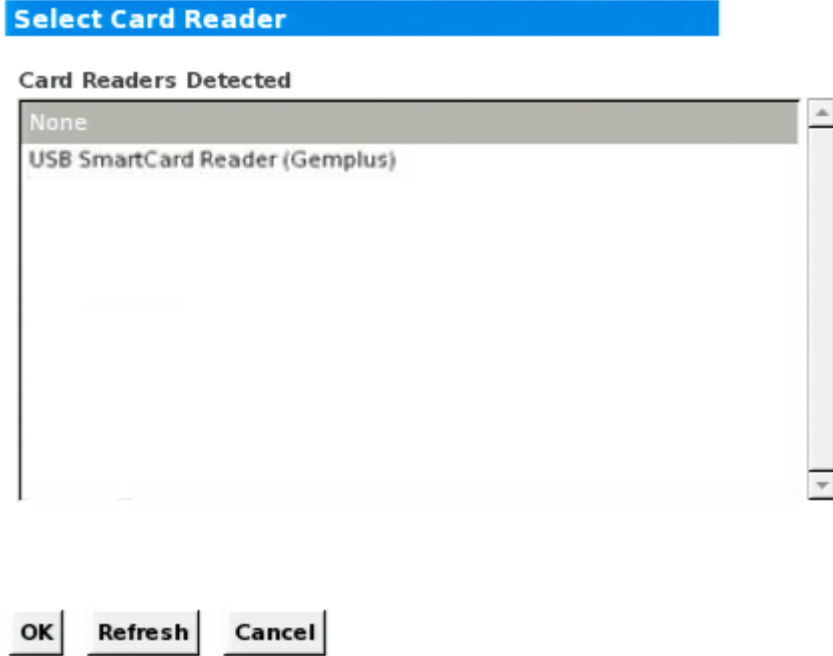
When the KVM session is terminated, either because it has been closed or because you switch to a new target, the smart card reader will be automatically unmounted from the target server.

► **To mount a smart card reader onto a target via the KX III Local console:**

1. Plug a USB smart card reader into the KX III using one of the USB ports located on the device. Once attached, the smart card reader will be detected by the KX III.
2. From the Local Console, click Tools.
3. Select the smart card reader from the Card Readers Detected list. Select None from the list if you do not want a smart card reader mounted.
4. Click OK. Once the smart card reader is added, a message will appear on the page indicating you have completed the operation successfully. A status of either Selected or Not Selected will appear in the left panel of the page under Card Reader.

► **To update the Card Readers Detected list:**

- Click Refresh if a new smart card has been mounted. The Card Readers Detected list will be refreshed to reflect the newly added smart card reader.



Local Console USB Profile Options

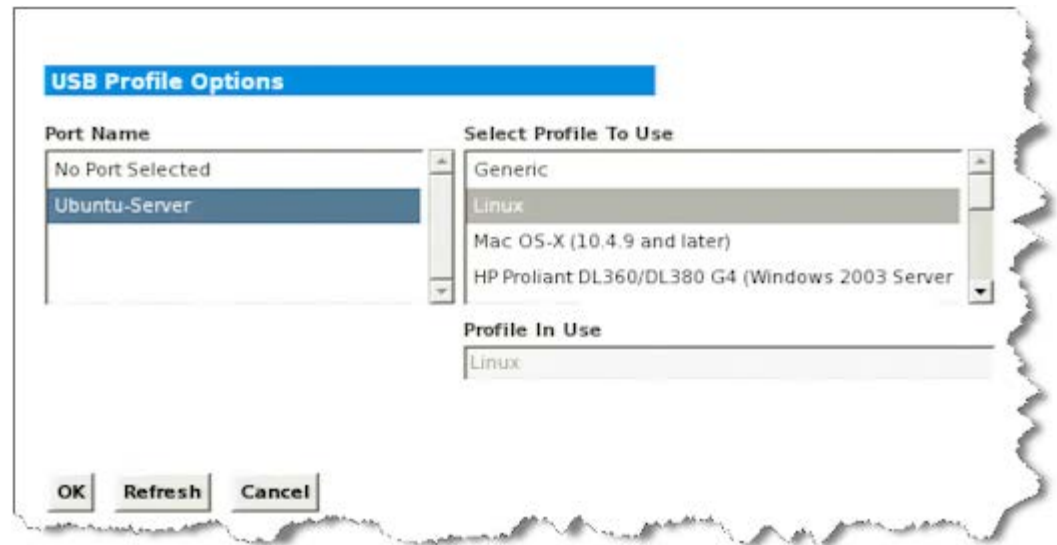
From the USB Profile Options section of the Tools page, you can choose from the available USB profiles.

The ports that can be assigned profiles are displayed in the Port Name field and the profiles that are available for a port appear in the Select Profile To Use field after the port is selected. The profiles selected for use with a port appear in the Profile In Use field.

► **To apply a USB profile to a local console port:**

1. In the Port Name field, select the port you want to apply the USB profile to.
2. In the Select Profile To Use field, select the profile to use from among those available for the port.

3. Click OK. The USB profile will be applied to the local port and will appear in the Profile In Use field.



KX III Local Console Factory Reset

Note: It is recommended that you save the audit log prior to performing a factory reset.

*The audit log is deleted when a factory reset is performed and the reset event is not logged in the audit log. For more information about saving the audit log, see **Audit Log** (on page 205).*

► To perform a factory reset:

1. Choose Maintenance > Factory Reset. The Factory Reset page opens.
2. Choose the appropriate reset option from the following options:
 - **Full Factory Reset**
Removes the entire configuration and resets the appliance completely to the factory defaults.
Note that any management associations with CommandCenter will be broken.
Because of the complete nature of this reset, you will be prompted to confirm the factory reset.
 - **Network Parameter Reset**
Resets the network parameters of the appliance back to the default values (click Device Settings > Network Settings to access this information).

3. Click Reset to continue. You will be prompted to confirm the factory reset because all network settings will be permanently lost.
4. Click OK proceed. Upon completion of full factory reset, the KX III device is automatically restarted.

Resetting the KX III Using the Reset Button on the Device

On the back panel of the device, there is a Reset button. It is recessed to prevent accidental resets (you need a pointed object to press this button).

The actions that are performed when the Reset button is pressed are defined on the Encryption & Share page. See **Encryption & Share** (see "**Encryption and Share**" on page 193).

Note: It is recommended that you save the audit log prior to performing a factory reset.

*The audit log is deleted when a factory reset is performed and the reset event is not logged in the audit log. For more information about saving the audit log, see **Audit Log** (on page 205).*

► To reset the device:

1. Power off the KX III.
2. Use a pointed object to press and hold the Reset button.
3. While continuing to hold the Reset button, power the KX III device back on.
4. Continue holding the Reset button for 10 seconds.



Appendix A Connecting a KX III and Cat5 Reach DVI - Provide Extended Local Port Functionality

An extended local port extends the reach of the local port beyond the rack the KX III is located, for example to another KVM switch.

This can be achieved by configuring a KX III to work with a Raritan Cat5 Reach DVI transmitter and receiver, which are then connected to a remote console or other device.

Once connected to the Cat5 Reach DVI, the KX III can be accessed up 500 feet (152 m) away.

Connecting the KX III to the Cat5 Reach DVI by daisy chaining Ethernet switches extends can extend the KX III's reach up to 3000 feet (914 m).

In This Chapter

About the Cat5 Reach DVI	398
Connect Cat5 Reach DVI and Cat5 Reach DVI	399

About the Cat5 Reach DVI

For details on the Cat5 Reach DVI, see the Cat5 Reach DVI online help available on the *Raritan Support page*
<http://www.raritan.com/support>.

Contact Raritan (<http://www.raritan.com/contact-us/>) for additional information on the Cat5 Reach DVI, or for information on purchasing.

Connect Cat5 Reach DVI and Cat5 Reach DVI

Note: The images used in the diagrams are not specific to Cat5 Reach DVI but the connections are accurate.

This section introduces three scenarios involving KVM switches.

- Connect the Cat5 Reach DVI between any KVM switch and its local console.
- Connect the Cat5 Reach DVI between two KVM switches.
- Connect the Cat5 Reach DVI between a computer/server and a KVM switch.

Turn off all devices before making the connections.

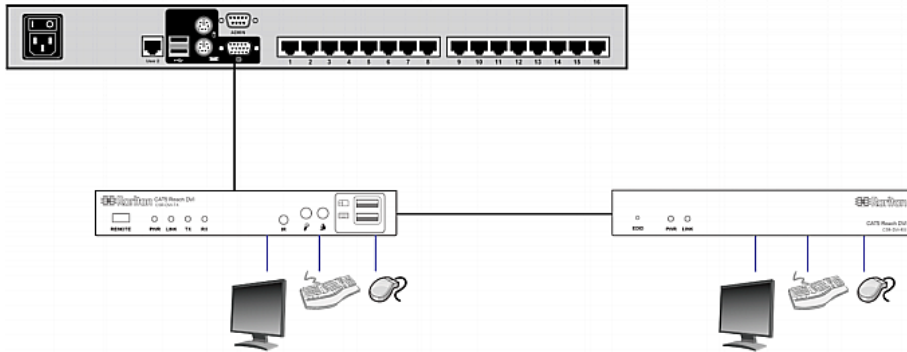
For detailed information on setting up the local and remote consoles, see **Connecting a Keyboard/Mouse/Video Source in Cat5 Reach DVI Help** for more information.

► **To connect Cat5 Reach DVI and Cat5 Reach DVI:**

1. If you have not already done so, set up the local and remote consoles with the Cat5 Reach DVI transmitter and receiver, respectively.
See **Basic Installation in Cat5 Reach DVI Help** for more information.
2. Use a Cat5e/6 cable to connect the transmitter and receiver.
3. Connect the transmitter and receiver to an appropriate power source respectively.
4. Connect the local console ports of the KVM switch to the transmitter.
 - a. Plug one end of the Raritan-provided DVI cable into the DVI-I IN port on the transmitter, and the other end into the KVM switch's video port.
 - b. Plug the USB-B connector of the Raritan-provided USB cable into the USB-B port on the transmitter, and the other end into the KVM switch's local USB-A port.

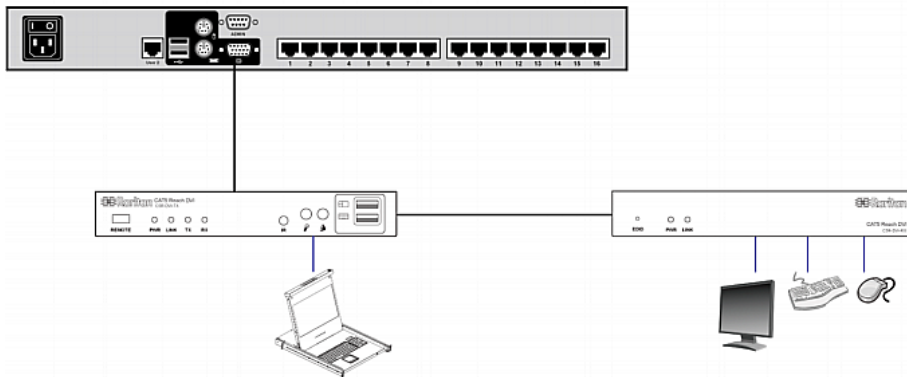
5. Turn on the KVM switch.

KVM



Tip: The local or remote console can be equipped with a KVM drawer instead of a set of keyboard, mouse and monitor. See the illustration below.

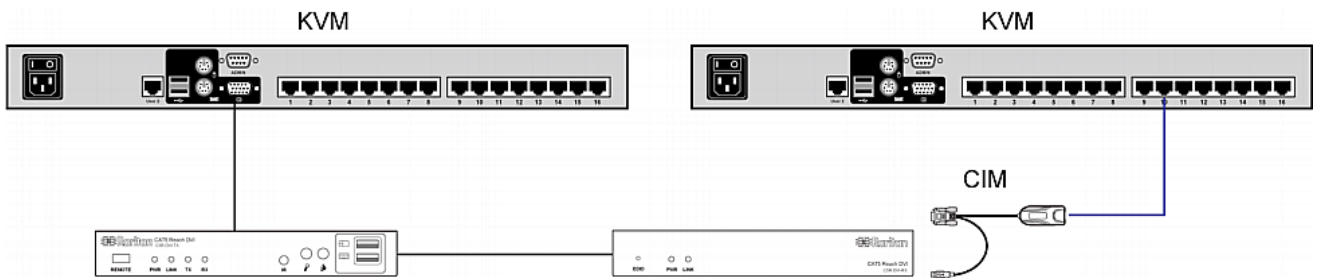
KVM



► To increase the distance between two tiered KVM switches:

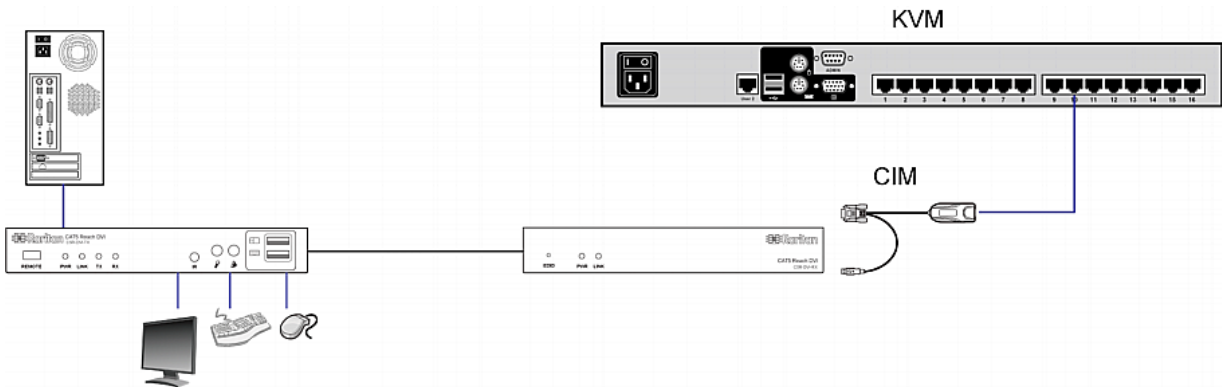
1. Set up a remote console by connecting the receiver to a KVM switch.
 - a. Connect a USB CIM to the receiver.
 - b. Connect this USB CIM to any channel port on the KVM switch via a Cat5 cable.
2. Use a Cat5e/6 cable to connect the transmitter and receiver.
3. Connect the transmitter and receiver to an appropriate power source respectively.
4. Connect the KVM switch to the transmitter.

5. Turn on both KVM switches.



► To increase the distance between any computer and a KVM switch:

1. Set up an optional local console with the transmitter.
2. Set up a remote console by connecting the receiver to a KVM switch.
3. Use a Cat5e/6 cable to connect the transmitter and receiver.
4. Connect the transmitter and receiver to an appropriate power source respectively.
5. Connect the computer to the transmitter.
6. Turn on the computer.



Appendix B Accessing a Paragon II from the KX III

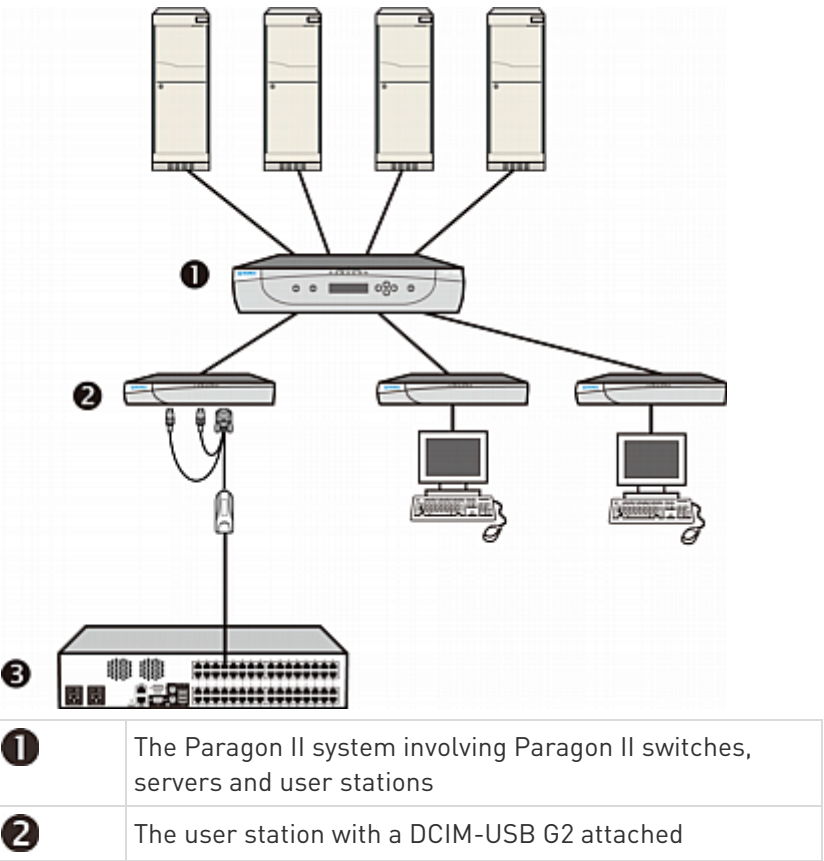
In This Chapter

Overview	402
Supported Paragon II CIMS and Configurations	403
Connecting the Paragon II to the KX III	408

Overview

Connect the Paragon II system to a KX III device that is managed by CC-SG so that Paragon II is accessible from CC-SG.
This diagram indicates the configuration integrating KX III.

Note: The images are for example purposes only, and may not look exactly like your device.



3	KX III

When you access the Paragon II system from KX III or CC-SG (if the KX III is managed by CC-SG), the Paragon II OSUI login screen appears for you to log in.

In this integration, you can perform any OSUI functions implemented with current Paragon II firmware or any KX III function implemented with current KX III firmware except for the virtual media feature.

When accessing the Paragon II OSUI through KX III, DO NOT attempt to synchronize the mouse manually. A mouse is not necessary on the OSUI screen and mouse synchronization will delay the keyboard response for seconds.

See ***Supported Paragon II CIMS and Configurations*** (on page 403) for additional information.

Supported Paragon II CIMS and Configurations

The KX III supports the P2CIM-APS2DUAL and P2CIM-AUSBDUAL CIMS, which provide two RJ45 connections to different KVM switches.

Support of these CIMS provides a second path to access the target in the event that one of the KVM switches is blocked or fails.

Paragon CIM	Supports	Does not support
P2CIM-APS2DUAL	- Servers with IBM® PS/2-type keyboard and mouse ports - Automatic skew compensation (when the CIMS are connected to Paragon II, not from a KX III) - Intelligent Mouse mode - Standard Mouse mode	- Virtual media - Smart cards - Absolute Mouse mode - Use with blade chassis - Cascaded KVM configurations

Paragon CIM	Supports	Does not support
P2CIM-AUSBDUAL	• Servers with USB- or Sun™ USB-type keyboard and mouse ports • Automatic skew compensation (when the CIMs are connected to Paragon II, not from a KX III) • Intelligent Mouse mode • Standard Mouse mode	• Virtual media • Smart cards • Absolute Mouse mode • Use with blade chassis • Cascaded KVM configurations

KX III-to-KX III Paragon CIM Guidelines

The following system configuration guidelines should be followed when you are using Paragon CIMs in a KX III-to-KX III configuration:

Concurrent Access

Both KX III KVM switches should be configured with the same policy for concurrent access to targets - both PC-Share or both Private.

If Private access to targets is required, both KVM switches must be configured accordingly:

- From Security > Security Settings > Encryption & Share, set PC Share Mode to 'Private'

This guarantees that concurrent access to targets is prohibited, for all targets by all user groups.

The KX III allows for more granular control of concurrent access to targets on a per user group basis. This is done by setting the user group's PC Share permissions. However, this is only enforced within the boundary of a KX III. User Group PC Share permissions must not be relied on if Privacy must be guaranteed when using the P2CIM-APS2DUAL or P2CIM-AUSB DUAL with the KX III.

CIM Name Updates

The P2CIM-APS2 and P2CIM-AUSB names are stored within the CIM's memory. There are two memory locations provided to accommodate the Paragon naming convention (12 characters) and the KX III naming convention (32 characters).

When first connected to a KX III, the Paragon name will be retrieved from memory and written into the CIM memory location used by KX III. Subsequent queries for the CIM name or updates to the CIM name from the KX III will be made to the memory location used by the KX III. Updates will not be made by the KX III to the memory location used by Paragon II.

When the CIM name is updated by one KX III, the other KX III will detect and retrieve the updated name on the next attempt to connect to that target. Until that time, the name will not be updated on the other KX III.

Port Status and Availability

The port status, displayed on the KX III Port Access page as either Up or Down, is updated to show whether the CIM is powered up and connected to the KX III port.

The port availability, as displayed on the KX III Port Access page as Idle, Busy or Connected, is only updated to reflect activity on a target that has been initiated from that same KX III.

If a connection to the target is in place from the other KX III, the availability is checked when a connection is attempted. Access is denied or allowed consistent with the PC-Share policy in place for the KX III. Until that time, the availability is not be updated on the other KX III.

If access is denied because the target is busy, a notification is displayed.

Working from CC-SG

Operations initiated from CC-SG are based on the Status, Availability and CIM name reported by the managed KX III. When the target is connected to two managed KX IIIs and the devices are added to CC-SG, two nodes will be created. Each node will have its own oob-kvm interface associated with it. Alternatively, a single node can be configured with an oob-kvm interface from each KX III.

If the KX IIIs are configured for 'Private' mode, when a second connection is attempted the user is notified that they cannot connect and access is denied.

When a port name change is initiated via the CC-SG Port Profile pane, the changed name is pushed to the managed KX III. The corresponding port name of the other KX III will not be updated in CC-SG until a connection is attempted to the target port via the other KX III's oob-kvm interface.

KX III-to-Paragon II Guidelines

The P2CIM-APS2DUAL or P2CIM-AUSBDUAL can be connected to a KX III and Paragon II.

Concurrent Access

The KX III and Paragon II must be configured with the same policy for concurrent access to targets.

Paragon II operation mode	Mode description	Supported?
Private	A server or other device on a specific channel port can be accessed exclusively by only one user at a time.	Supported. Paragon II and the KX III must be set to Private. The Private setting is applied on to KX III device, not per user group. The Paragon II uses Red to indicate 'busy' or Green to indicate 'available'.
PC Share	A server or other device on a specific channel	Supported. However, PC Share Idle

Paragon II operation mode	Mode description	Supported?
	port can be selected and controlled by more than one user, but only one user has keyboard and mouse control at any one time.	Timeout, which is configured on the Paragon II, is not supported. Both users will have concurrent keyboard and mouse control. The Paragon II uses Green to indicate 'available'. This will also be true if another user is already accessing the target.
Public View	While one user is accessing a server or other device on a specific channel port, other users can select that channel port and view the video output from that device. However, only the first user will have keyboard and mouse control until they disconnect or switch away.	Not supported. This mode cannot be used when connecting the CIM to a Paragon II and the KX III. The Paragon II uses Yellow to indicate it is in P-View mode.

CIM Name Updates

- CIM names updated from Paragon II are stored and retrieved from the CIM memory location corresponding to the Paragon naming convention.
- CIM names updated from the KX III are stored and retrieved from the CIM memory location corresponding to the KX III naming convention.
- CIM name updates do not propagate between the Paragon II and the KX III.

Supported Connection Distances Between Paragon II and KX III

When using KX III as the front end of a Paragon II system, you should restrict the cable length (distance) for good video quality.

Supported distance from the Paragon II user station to the target server is 500 cable feet (152 m). Greater distances may result in video performance that may or may not be acceptable to you.

Supported distance from KX III to the Paragon II user station is up to 150 cable feet (45 m).

Connecting the Paragon II to the KX III

► **To connect the Paragon II system to a KX III:**

1. Check whether the Paragon II user station that you want to connect to the KX III is implemented with version 4.6 firmware (or later). If not, upgrade it.

The Paragon II user station can be one of these:

- P2-UST
- P2-EUST
- P2-EUST/C

See **Paragon II Help** for information on upgrading.

2. Plug a compatible DCIM-USB into the USB and video ports on the Paragon II user station.

If the system is a two- or three-tier system, ensure the Paragon II user station is connected to the base KX III device (first tier).

3. Connect the Paragon II user station to a KX III device via a Cat5 UTP cable up to 150 feet (45 m).
 - Plug one end of the cable to the DCIM's RJ-45 port and the other end to one of the channel ports on the KX III device.
4. If you want to have more paths to access the same Paragon II system in KX III or CC-SG, repeat Steps 1 to 3 to connect additional user stations to the KX III.

Appendix C Updating the LDAP Schema

In This Chapter

Returning User Group Information	409
Setting the Registry to Permit Write Operations to the Schema	410
Creating a New Attribute	410
Adding Attributes to the Class.....	411
Updating the Schema Cache	413
Editing rcusergroup Attributes for User Members.....	413

Returning User Group Information

Use the information in this section to return User Group information (and assist with authorization) once authentication is successful.

From LDAP/LDAPS

When an LDAP/LDAPS authentication is successful, the KX III determines the permissions for a given user based on the permissions of the user's group. Your remote LDAP server can provide these user group names by returning an attribute named as follows:

rcusergroup attribute type: string

This may require a schema extension on your LDAP/LDAPS server. Consult your authentication server administrator to enable this attribute. In addition, for Microsoft® Active Directory®, the standard LDAP memberOf is used.

From Microsoft Active Directory

Note: This should be attempted only by an experienced Active Directory® administrator.

Returning user group information from Microsoft's® Active Directory for Windows 2000® operating system server requires updating the LDAP/LDAPS schema. See your Microsoft documentation for details.

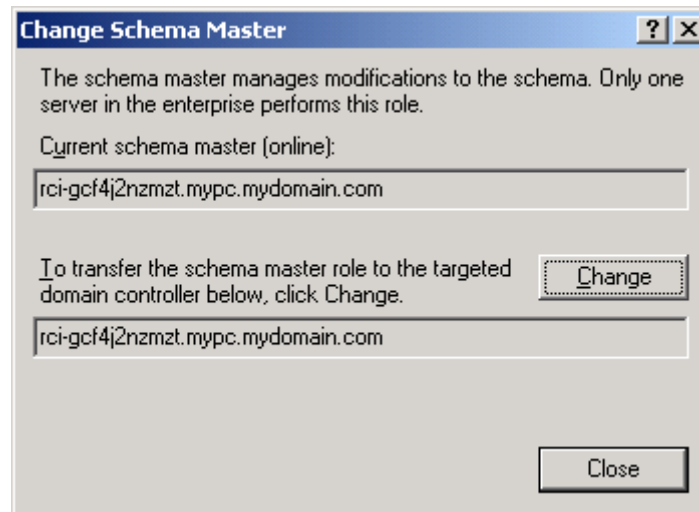
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

► **To permit write operations to the schema:**

1. Right-click the Active Directory® Schema root node in the left pane of the window and then click Operations Master. The Change Schema Master dialog appears.



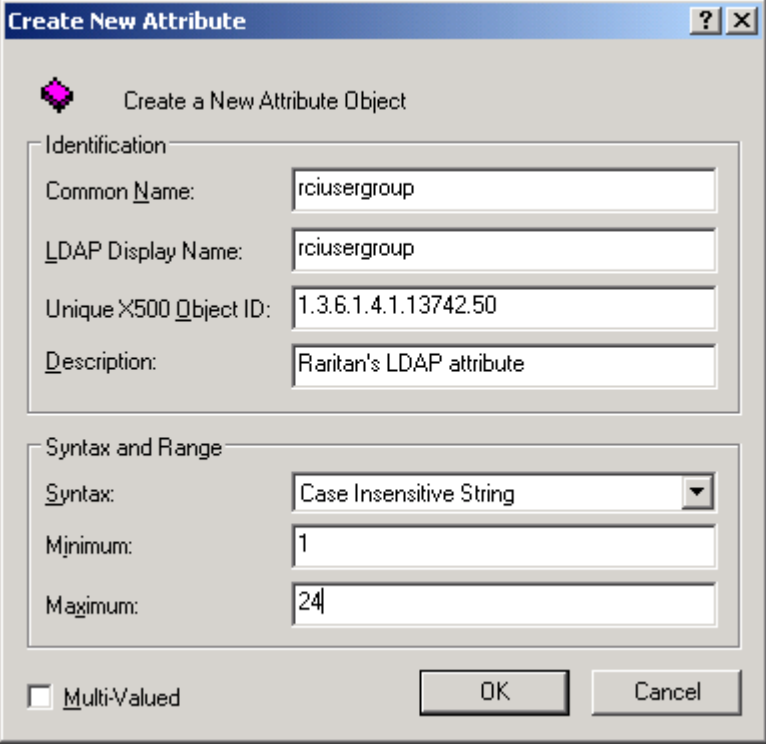
2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**
3. Click OK.

Creating a New Attribute

► **To create new attributes for the rcigroup class:**

1. Click the + symbol before Active Directory® Schema in the left pane of the window.
2. Right-click Attributes in the left pane.

- Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.



The image shows a Windows-style dialog box titled "Create New Attribute". It has a blue title bar with a question mark icon and a close button. The main area is light gray and contains two sections: "Identification" and "Syntax and Range".

Identification section:

- Common Name:** Text box containing "rciusergroup".
- LDAP Display Name:** Text box containing "rciusergroup".
- Unique X500 Object ID:** Text box containing "1.3.6.1.4.1.13742.50".
- Description:** Text box containing "Raritan's LDAP attribute".

Syntax and Range section:

- Syntax:** A drop-down menu showing "Case Insensitive String".
- Minimum:** Text box containing "1".
- Maximum:** Text box containing "24".

At the bottom left, there is a checkbox labeled "Multi-Valued" which is currently unchecked. At the bottom right, there are two buttons: "OK" and "Cancel".

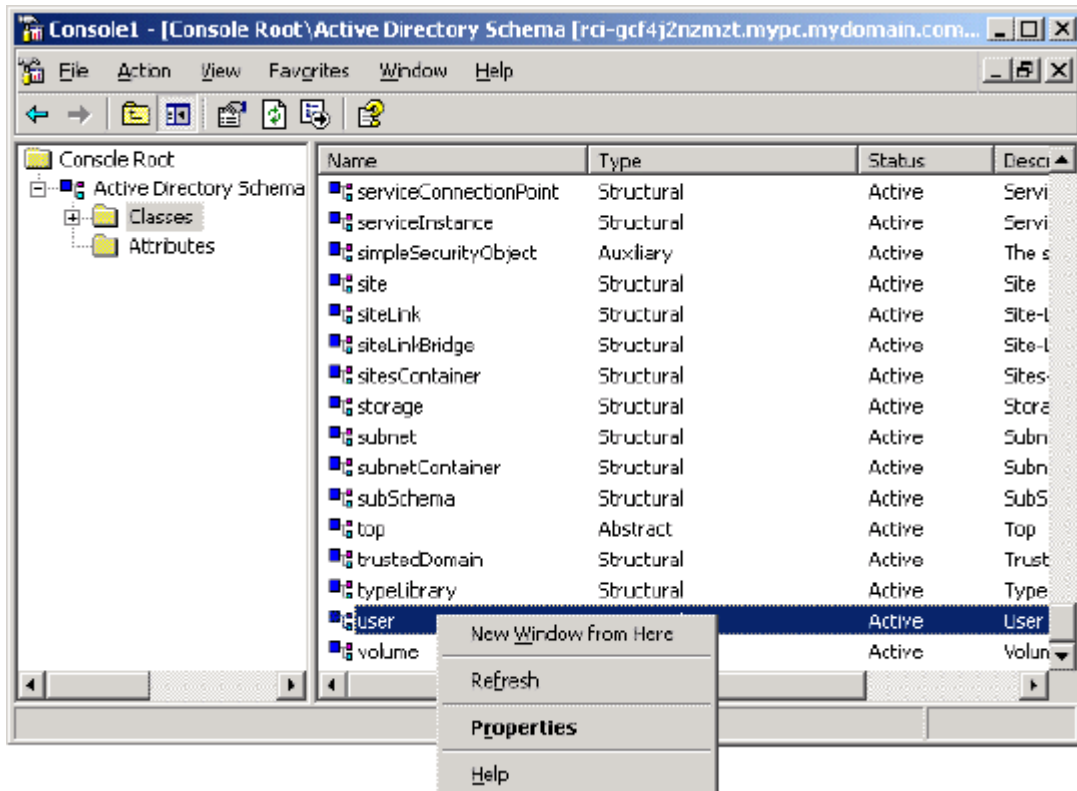
- Type *rciusergroup* in the Common Name field.
- Type *rciusergroup* in the LDAP Display Name field.
- Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
- Type a meaningful description in the Description field.
- Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
- Type *1* in the Minimum field.
- Type *24* in the Maximum field.
- Click OK to create the new attribute.

Adding Attributes to the Class

► To add attributes to the class:

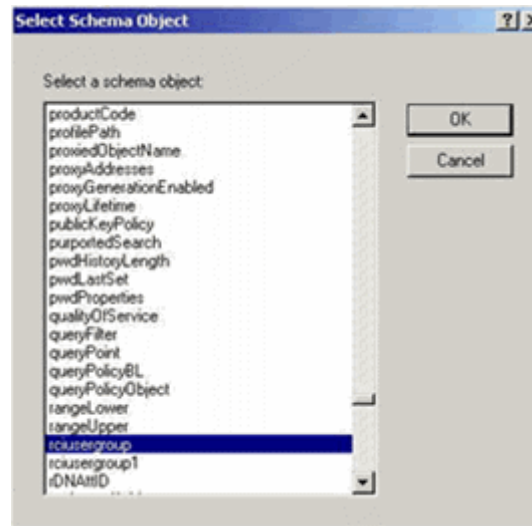
- Click Classes in the left pane of the window.

2. Scroll to the user class in the right pane and right-click it.



3. Choose Properties from the menu. The user Properties dialog appears.
4. Click the Attributes tab to open it.
5. Click Add.

- Choose rcigroup from the Select Schema Object list.



- Click OK in the Select Schema Object dialog.
- Click OK in the User Properties dialog.

Updating the Schema Cache

► **To update the schema cache:**

- Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.
- Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

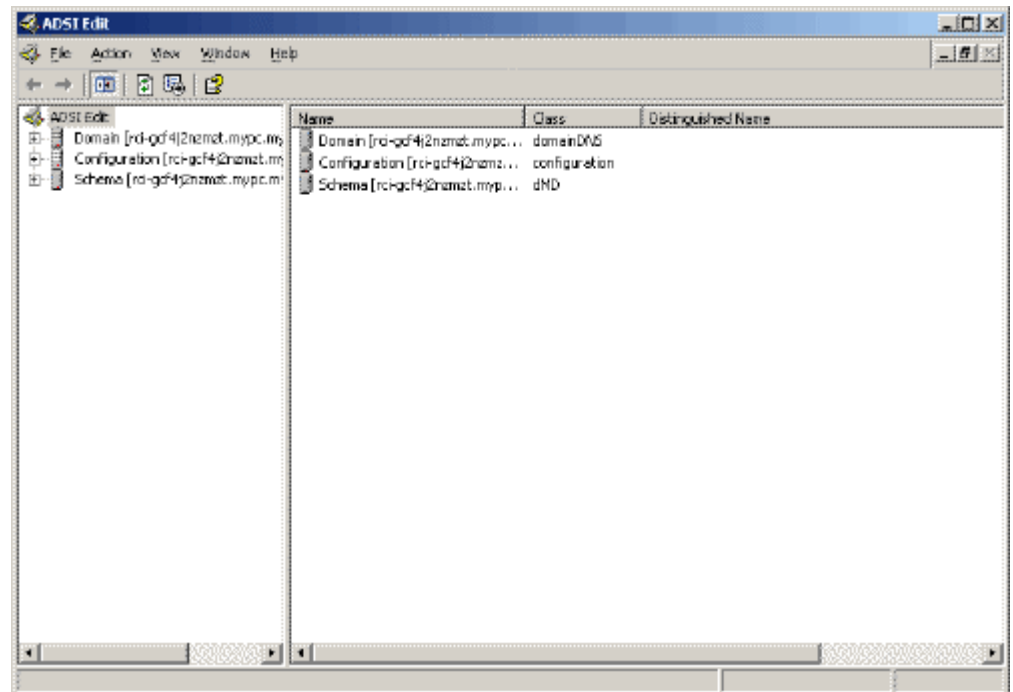
Editing rcigroup Attributes for User Members

To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

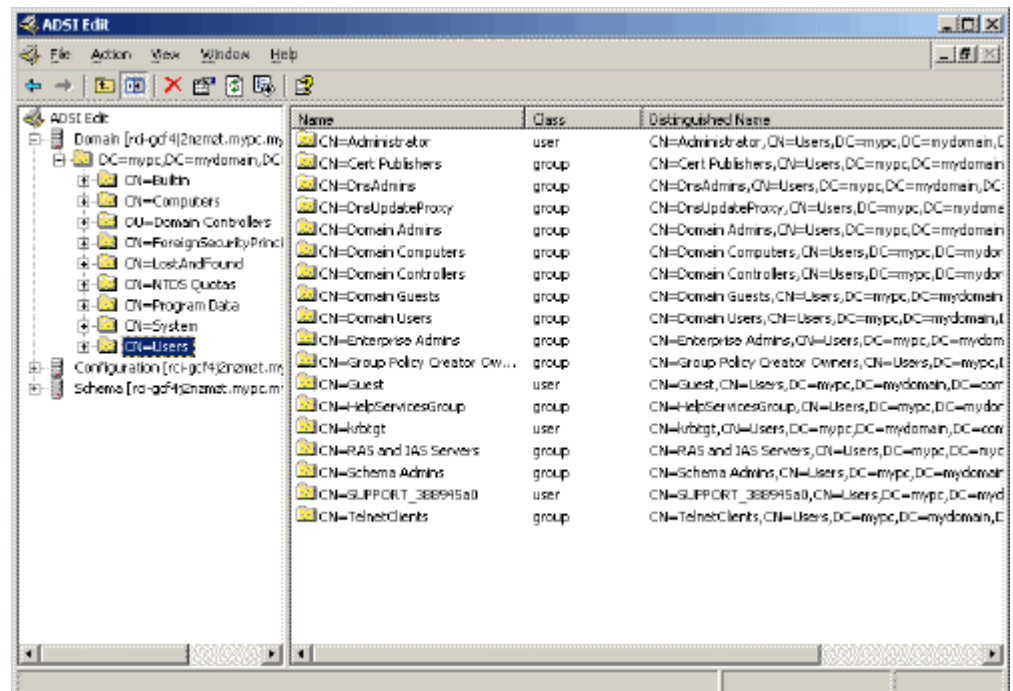
► **To edit the individual user attributes within the group rcigroup:**

- From the installation CD, choose Support > Tools.
- Double-click SUPTOOLS.MSI to install the support tools.

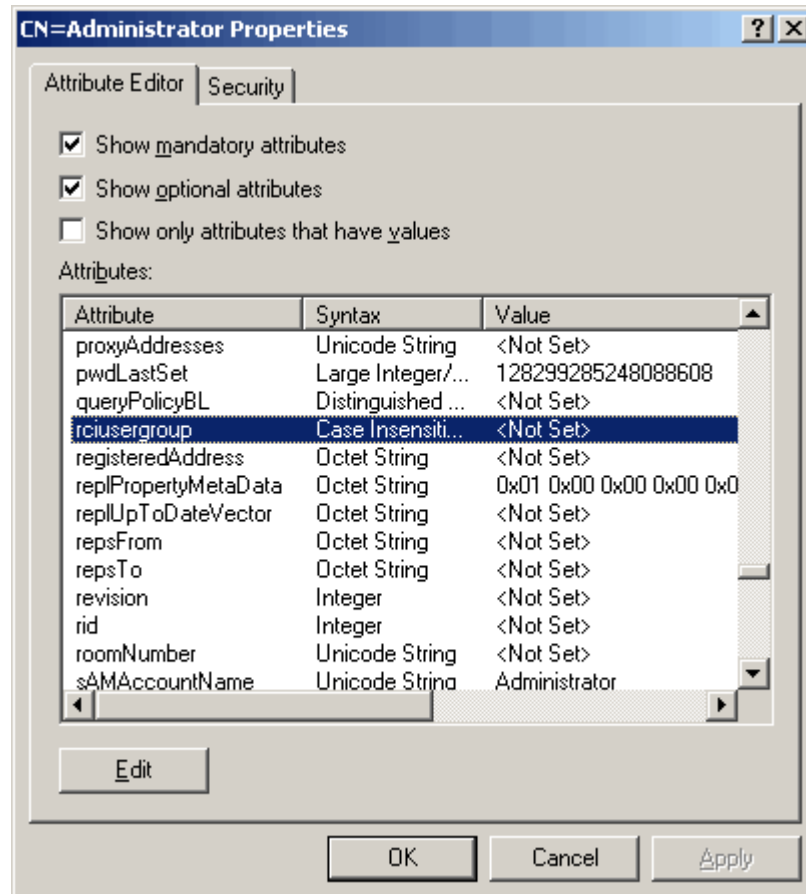
- Go to the directory where the support tools were installed. Run `adsiedit.msc`. The ADSI Edit window opens.



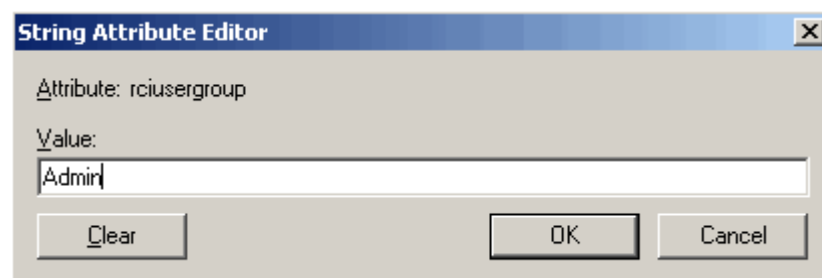
- Open the Domain.
- In the left pane of the window, select the CN=Users folder.



6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.
7. Click the Attribute Editor tab if it is not already open. Choose rcusergroup from the Attributes list.



8. Click Edit. The String Attribute Editor dialog appears.
9. Type the user group (created in the KX III) in the Edit Attribute field. Click OK.



Appendix D Specifications

In This Chapter

Hardware	416
Software.....	438
BSMI Certification	443

Hardware

KX III Dimensions and Physical Specifications

Dominion KX III model	Description	Power & heat dissipation	Dimensions (WxDxH)	Weight	Operating temp	Humidity
DKX3-108	8 server ports 1 remote user 1 local port for use at the rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73"	8.60lbs	0° - 45° C	0-85 % RH
			439x334x44 mm	3.9kg	32° - 113° F	
DKX3-116	16 server ports 1 remote user 1 local port for use at the rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73"	8.60lbs	0° - 45° C	0-85 % RH
			439x334x44 mm	3.9kg	32° - 113° F	
DKX3-132	32 server ports 1 remote user 1 local port for use at the rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73"	8.60lbs	0° - 45° C	0-85 % RH
			439x334x44 mm	3.9kg	32° - 113° F	
DKX3-216	16 server	Dual Power 110V/240V,	17.3" x 13.15" x	9.08lbs	0° - 45° C	0-85 % RH

Dominion KX III model	Description	Power & heat dissipation	Dimensions (WxDxH)	Weight	Operating temp	Humidity
	ports	50-60Hz	1.73"			
	2 remote users 1 local port for use at the rack	1.8A 60W 52 KCAL	439x334x44 mm	4.12kg	32° - 113° F	
DKX3-232	32 server ports 2 remote users 1 local port for use at the rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73"	9.08lbs	0° - 45° C	0-85 % RH
			439x334x44 mm	4.12kg	32° - 113° F	
DKX3-416	16 server ports 4 remote users 1 local port for use at the rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73"	9.08lbs	0° - 45° C	0-85 % RH
			439x334x44 mm	4.12kg	32° - 113° F	
DKX3-432	32 server ports 4 remote users 1 local port for use at the rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73"	9.08lbs	0° - 45° C	0-85 % RH
			439x334x44 mm	4.12kg	32° - 113° F	
DKX3-464	64 server ports 4 remote users 1 local port for use at	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.3" x 3.5"	12.39lbs	0° - 45° C	0-85 % RH
			439x338x89 mm	5.62kg	32° - 113° F	

Dominion KX III model	Description	Power & heat dissipation	Dimensions (WxDxH)	Weight	Operating temp	Humidity
	the rack					
DKX3-808	8 server ports 8 remote users 1 local port for use at the rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73"	9.96lbs	0° - 45° C	0-85 % RH
			439x334x44 mm	4.52kg	32° - 113° F	
DKX3-832	32 server ports 8 remote users 1 local port for use at the rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.15" x 1.73"	9.96lbs	0° - 45° C	0-85 % RH
			439x334x44 mm	4.52kg	32° - 113° F	
DKX3-864	64 server ports 8 remote users 1 local port for use at the rack	Dual Power 110V/240V, 50-60Hz 1.8A 60W 52 KCAL	17.3" x 13.3" x 3.5"	12.39lbs	0° - 45° C	0-85 % RH
			439x338x89 mm	5.62kg	32° - 113° F	

KX III Supported Target Server Video Resolutions

When using digital CIMS, you set the target's video resolution to match your monitor's native display resolution. The native display resolution is set when configuring ports for digital CIMS (see *Configure the CIM Target Settings* (on page 103)).

Following is a complete list of KX III supported video resolutions when accessing a target from the Remote Console.

- 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
- 1920x1200@60Hz (Requires Reduced Blanking Time)

For 1920x1200@60Hz, you must use a digital CIM and set the CIM's preferred resolution to 1920x1200@60Hz.

KX III Supported Local Port DVI Resolutions

Following are the resolutions supported when connecting to a DVI monitor from the Local port.

- 1920x1080@60Hz
- 1280x720@60Hz
- 1024x768@60Hz (default)
- 1024x768@75Hz
- 1280x1024@60Hz
- 1280x1024@75Hz
- 1600x1200@60Hz
- 800x480@60Hz
- 1280x768@60Hz
- 1366x768@60Hz
- 1360x768@60Hz
- 1680x1050@60Hz
- 1440x900@60Hz

Target Server Video Resolution Supported Connection Distances and Refresh Rates

The maximum supported distance is a function of many factors including the type/quality of the Cat5 cable, server type and manufacturer, video driver and monitor, environmental conditions, and user expectations.

The following table summarizes the maximum target server distance for various video resolutions and refresh rates:

Target server video resolution	Maximum distance
1024x768@60Hz (and below)	150' (45 m)
1280x1024@60Hz	100' (30 m)
1280x720@60Hz	75' (22 m)
1600x1200@60Hz	50' (15 m)
1920x1080@60Hz	50' (15 m)

See **KX III Supported Target Server Video Resolutions** (on page 419) for the video resolutions supported by the KX III.

Note: Due to the multiplicity of server manufacturers and types, OS versions, video drivers, and so on, as well as the subjective nature of video quality, Raritan cannot guarantee performance across all distances in all environments.

Supported Computer Interface Module (CIMs) Specifications

Digital CIMs support Display Data Channels (DDC) and Enhanced Extended Display Identification Data (E-EDID).

Note: Both plugs must be plugged in for the HDMI and DVI CIMs.

CIM model	Description	Dimensions (WxDxH)	Weight
D2CIM-DVUSB	Dual USB CIM for: - OS virtual media - Smartcard/CAC - Audio - Absolute Mouse Synchronization	1.7" x 3.5" x 0.8" 43 x 90 x 19mm	0.25lb 0.11kg

CIM model	Description	Dimensions (WxDxH)	Weight
			
D2CIM-VUSB	USB CIM for: - OS virtual media - Absolute Mouse Synchronization 	1.3" x 3.0" x 0.6" 33 x 76 x 15mm	0.20lb 0.09kg
D2CIM-DVUSB-DP	Digital CIM that provides digital-to-analog conversion and support for: - OS virtual media - Smartcard/CAC - Audio - Absolute and Relative Mouse Synchronization 	1.7" x 3.5" x 0.8" 43 x 90 x 19mm	0.25lb 0.11kg

CIM model	Description	Dimensions (WxDxH)	Weight
D2CIM-DVUSB-HDMI	Digital CIM that provides digital-to-analog conversion and support for: - OS virtual media - Smartcard/CAC - Audio - Absolute and Relative Mouse Synchronization 	1.7" x 3.5" x 0.8" 43 x 90 x 19mm	0.25lb 0.11kg
D2CIM-DVUSB-DVI	Digital CIM that provides digital-to-analog conversion and support for: - OS virtual media - Smartcard/CAC - Audio - Absolute and Relative Mouse Synchronization 	1.7" x 3.5" x 0.8" 43 x 90 x 19mm	0.25lb 0.11kg

CIM model	Description	Dimensions (WxDxH)	Weight
DCIM-PS2	CIM for PS2 	1.3" x 3.0" x 0.6" 33 x 76 x 15mm	0.20lb 0.09kg
DCIM-USBG2	CIM for USB and Sun USB 	1.3" x 3.0" x 0.6" 33 x 76 x 15mm	0.20lb 0.09kg

Supported Digital Video CIMs for Mac

Use a digital video CIM to connect to the following Mac® ports:

Mac port	CIM
DVI	D2CIM-DVUSB-DVI
HDMI	D2CIM-DVUSB-HDMI
DisplayPort or Thunderbolt	D2CIM-DVUSB-DP

If the Mac's HDMI or DisplayPort video has a mini connector, a passive adapter cable may be required to connect to the full sized HDMI and DisplayPort plugs on the digital CIMs.

Alternatively, use the Mac VGA adapter with the D2CIM-VUSB or D2CIM-DVUSB. Note that this may be less reliable and the video quality may suffer.

For information on established modes supported by the KX III 2.5.0 (and later) for Mac, see ***Digital CIM Established and Standard Modes*** (on page 425).

Digital CIM Timing Modes

Following are the default timing modes that are used when the KX III communicates with a video source via a digital CIM.

The timing mode that is used is dependent on the native resolution of the video source.

- 1024x768@60Hz
- 1152x864@60Hz
- 1280x720@60Hz
- 1280x960@60Hz
- 1280x1024@60Hz (default resolution applied to digital CIMs)
- 1360x768@60Hz
- 1400x1050@60Hz
- 1440x900@60Hz
- 1600x1200@60Hz
- 1680x1050@60Hz
- 1920x1080@60Hz
- 1920x1200@60Hz

See *Configuring CIM Ports* (on page 102) in online help for more information.

Digital CIM Established and Standard Modes

The following additional established and standard resolutions and timing modes are supported by the KX III 3.0.0 (and later).

Digital CIM Established Modes

- 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

Digital CIM Standard Modes

- 1152x864@75Hz VESA
- 1280x960@60Hz VESA
- 1280x1024@60Hz VESA
- 1360x768@60Hz VESA
- 1400x1050@60Hz VESA
- 1440x900@60Hz VESA
- 1600x1200 @60Hz VESA
- 1680x1050@60Hz VESA
- 1920x1080@60Hz VESA

DVI Compatibility Mode

DVI Compatibility Mode may be required if you are using an HDMI CIM to connect to a Dell Optiplex target with an Intel video card, or a Mac® Mini with an HDMI video port.

Selecting this mode ensures a good video quality from the targets.

See ***Configuring CIM Ports*** (on page 102) in online help.

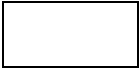
Supported Remote Connections

Remote connection	Details
Network	10BASE-T, 100BASE-T, and 1000BASE-T (Gigabit) Ethernet
Protocols	TCP/IP, UDP, SNMP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

Network Speed Settings

KX III network speed setting						
Network switch port setting	Auto	1000/Full	100/Full	100/Half	10/Full	10/Half
Auto	Highest Available Speed	1000/Full	KX III: 100/Full Switch: 100/Half	100/Half	KX III: 10/Full Switch: 10/Half	10/Half
1000/Full	1000/Full	1000/Full	No Communication	No Communication	No Communication	No Communication
100/Full	KX III: 100/Half Switch: 100/Full	KX III: 100/Half Switch: 100/Full	100/Full	KX III: 100/Half Switch: 100/Full	No Communication	No Communication
100/Half	100/Half	100/Half	KX III: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
10/Full	KX III: 10/Half Switch: 10/Full	No Communication	No Communication	No Communication	10/Full	KX III: 10/Half Switch: 10/Full
10/Half	10/Half	No Communication	No Communication	No Communication	KX III: 10/Full Switch: 10/Half	10/Half

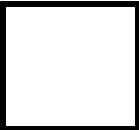
Legend:

 Does not function as expected

 Supported

 Functions; not recommended

 NOT supported by Ethernet specification; product will communicate, but collisions will occur

 Per Ethernet specification, these should be “no communication,” however, note that the KX III behavior deviates from expected behavior

Note: For reliable network communication, configure the KX III and the LAN switch to the same LAN Interface Speed and Duplex. For example, configure the KX III and LAN Switch to Autodetect (recommended), or set both to a fixed speed/duplex such as 100MB/s/Full.

Dell Chassis Cable Lengths and Video Resolutions

In order to maintain video quality, Raritan recommends using the following cable lengths and video resolutions when you are connecting to Dell® blade chassis from the KX III:

Video resolution	Cable length
1024x768@60Hz	50' (15.24 m)
1280x1024@60Hz	50' (15.24 m)
1600x1200@60Hz	30' (9.14 m)

Smart Card Minimum System Requirements

Local Port Requirements

The basic interoperability requirement for local port attachment to the KX III is:

- All devices (smart card reader or token) that are locally attached must be USB CCID-compliant.

Target Server Requirements

When using smart card readers, the basic requirements for interoperability at the target server are:

- The IFD (smart card reader) Handler must be a standard USB CCID device driver (comparable to the generic Microsoft® USB CCID driver).
- A digital CIM or D2CIM-DVUSB (Dual-VM CIM) is required and must be using firmware version 3A6E or later.
- Blade chassis server connections, where a CIM per blade is used, are supported.
- Blade chassis server connections, where a CIM per chassis is used, is only supported for IBM® BladeCenter® models H and E with auto-discovery enabled.

Windows XP Targets

Windows XP® operating system targets must be running Windows XP SP3 in order to use smart cards with the KX III.

Linux Targets

If you are using a Linux® target, the following requirements must be met to use smart card readers with the Raritan device.

- CCID Requirements
If the Raritan D2CIM-DVUSB VM/CCID is not recognized as a smart card reader by your Linux target, you may need to update the CCID driver version to 1.3.8 or above and update the driver configuration file (Info.plist).

Operating system	CCID requirements
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

Remote Client Requirements

The basic requirements for interoperability at the remote client are:

- The IFD (smart card reader) Handler must be a PC/SC compliant device driver.
- The ICC (smart card) Resource Manager must be available and be PC/SC compliant.
- The JRE® Java™ 1.7 with smart card API must be available for use by the Raritan client application.

Remote Linux Client Requirements

If you are using a Linux® client, the following requirements must be met to use smart card readers with the Raritan device.

Note: User login to client, on smart card insertion, may take longer when 1 or more KVM sessions are actively in place to targets. As the login process to these targets is also under way.

- PC/SC Requirements

Operating system	Required PC/SC
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

- Create a Java® Library Link
A soft link must be created to the libpcsc-lite.so after upgrading RHEL 4, RHEL 5 and FC 10. For example, `ln -s /usr/lib/libpcsc-lite.so.1 /usr/lib/libpcsc-lite.so`, assuming installing the package places the libraries in /usr/lib or /user/local/lib
- PC/SC Daemon
When the pcsc daemon (resource manager in framework) is restarted, restart the browser

Supported Smart Card Readers

Type	Vendor	Model	Verified
USB	SCM Microsystems	SCR331	Verified on local and remote

Type	Vendor	Model	Verified
USB	SCM Microsystems	SCR331	Verified on local and remote
USB	ActivIdentity®	ActivIdentity USB Reader v2.0	Verified on local and remote
USB	ActivIdentity	ActivIdentity USB Reader v3.0	Verified on local and remote
USB	Gemalto®	GemPC USB-SW	Verified on local and remote
USB Keyboard/Card reader combo	Dell®	USB Smart Card Reader Keyboard	Verified on local and remote
USB Keyboard/Card reader combo	Cherry GmbH	G83-6744 SmartBoard	Verified on local and remote
USB reader for SIM-sized cards	Omniquey	6121	Verified on local and remote
Integrated (Dell Latitude D620)	O2Micro	OZ776	Remote only
PCMCIA	ActivIdentity	ActivIdentity PCMCIA Reader	Remote only
PCMCIA	SCM Microsystems	SCR243	Remote only

Note: SCM Microsystems SCR331 smart card readers must be using SCM Microsystems firmware v5.25.

Unsupported Smart Card Readers

This table contains a list of readers that Raritan has tested and found not to work with the Raritan device, therefore they are unsupported.

If a smart card reader does not appear in the supported smart card readers table or in the unsupported smart card readers table, Raritan cannot guarantee it will function with the device.

Type	Vendor	Model	Notes
USB Keyboard/Card reader Combo	HP®	ED707A	No interrupt endpoint => not compatible with Microsoft® driver
USB Keyboard/Card reader Combo	SCM Microsystems	SCR338	Proprietary card reader implementation (not

Type	Vendor	Model	Notes
			CCID-compliant)
USB Token	Aladdin®	eToken PRO™	Proprietary implementation

Audio Playback and Capture Recommendations and Requirements

Audio Level

- Set the target audio level to a mid-range setting.
For example, on a Windows® client, set the audio to 50 or lower.

This setting must be configured through the playback or capture audio device, not from the client audio device control.

Recommendations for Audio Connections when PC Share Mode is Enabled

If you are using the audio feature while running PC Share mode, audio playback and capture are interrupted if an additional audio device is connected to the target.

For example, User A connects a playback device to Target1 and runs an audio playback application then User B connects a capture device to the same target. User A's playback session is interrupted and the audio application may need to be restarted.

The interruption occurs because the USB device needs to be re-enumerated with the new device configuration.

It may take some time for the target to install a driver for the new device.

Audio applications may stop playback completely, go to the next track, or just continue playing.

The exact behavior is dependent on how the audio application is designed to handle a disconnect/reconnect event.

Bandwidth Requirements

The table below details the audio playback and capture bandwidth requirements to transport audio under each of the selected formats.

Audio format	Network bandwidth requirement
44.1 KHz, 16bit stereo	176 KB/s
44.1 KHz, 16bit mono	88.2 KB/s

Audio format	Network bandwidth requirement
2.05 KHz, 16bit stereo	88.2 KB/s
22.05 KHz, 16bit mono	44.1 KB/s
11.025 KHz, 16bit stereo	44.1 KB/s
11.025 KHz, 16bit mono	Audio 22.05 KB/s

In practice, the bandwidth used when an audio device connects to a target is higher due to the keyboard and video data consumed when opening and using an audio application on the target.

A general recommendation is to have at least a 1.5MB connection before running playback and capture.

However, high video-content, full-color connections using high-target screen resolutions consume much more bandwidth and impact the quality of the audio considerably.

To help mitigate quality degeneration, there are a number of recommended client settings that reduce the impact of video on audio quality at lower bandwidths:

- Connect audio playback at the lower quality formats. The impact of video consuming bandwidth is much less notable at 11k connections than at 44k
- Set the connection speed under Connection Properties to a value that best matches the client to server connection
- Under Connection Properties, set the color depth to as low a value as possible. Reducing the color depth to 8 bit color considerably reduces the bandwidth consumed
- Set Smoothing, to High. This will improve the appearance of the target video by reducing displayed video noise
- Under Video settings, set the Noise Filter to its highest setting of 7 (highest value) so less bandwidth is used for target screen changes

Audio in a Mac Environment

Following are known issues in a Mac® environment.

- On Mac clients, only one playback device is listed on the Connect Audio panel when accessing the device through the Virtual KVM Client (VKC). The device listed is the default and is displayed on the Connect Audio panel as Java Sound Audio Engine.
- Using audio on a Mac target through Skype® may cause the audio to be corrupted.

Number of Supported Audio/Virtual Media and Smartcard Connections

Following are the number of simultaneous Audio/Virtual Media and Smartcard connections that can be made from a client to a target:

- 1 smartcard
- 1 virtual media
- 1 Smartcard and 1 virtual media
- 2 virtual media

Certified Modems

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

KX III Supported Keyboard Languages

The KX III provides keyboard support for the languages listed in the following table.

*Note: You can use the keyboard for Chinese, Japanese, and Korean for display only; local language input is not supported at this time for the KX III Local Console functions. For more information about non-US keyboards, see **Informational Notes** (on page 444).*

Note: Raritan strongly recommends that you use system-config-keyboard to change languages if you are working in a Linux environment.

Language	Regions	Keyboard layout
US English	United States of America and most of English-speaking countries: for example, Canada, Australia, and New Zealand.	US Keyboard layout
US English International	United States of America and most of English-speaking countries: for example, Netherlands	US Keyboard layout
UK English	United Kingdom	UK layout keyboard
Chinese	Hong Kong S. A. R., Republic of	Chinese Traditional

Language	Regions	Keyboard layout
Traditional	China (Taiwan)	
Chinese Simplified	Mainland of the People's Republic of China	Chinese Simplified
Korean	South Korea	Dubeolsik Hangul
Japanese	Japan	JIS Keyboard
French	France	French (AZERTY) layout keyboard.
German	Germany and Austria	German keyboard (QWERTZ layout)
French	Belgium	Belgian
Norwegian	Norway	Norwegian
Danish	Denmark	Danish
Swedish	Sweden	Swedish
Hungarian	Hungary	Hungarian
Slovenian	Slovenia	Slovenian
Italian	Italy	Italian
Spanish	Spain and most Spanish speaking countries	Spanish
Portuguese	Portugal	Portuguese

Mac Mini BIOS Keystroke Commands

The following BIOS commands have been tested on Intel-based Mac® Mini target servers and Mac Lion® servers running Mac Snow Leopard®. The servers were attached to a KX III with D2CIM-DVUSB and D2CIM-VUSB CIMS. See below for the supported keys and any notes.

Keystroke	Description	Virtual Media CIM	Dual Virtual Media CIM	Mac Lion Server HDMI CIM
Press C during startup	Start up from a bootable CD or DVD, such as the Mac OS X Install disc	Yes	Yes	Yes

Keystroke	Description	Virtual Media CIM	Dual Virtual Media CIM	Mac Lion Server HDMI CIM
Press D during startup	Start up in Apple Hardware Test (AHT)	Yes May need BIOS Mac profile for the mouse to work	Yes May need BIOS Mac profile for the mouse to work	Yes May need BIOS Mac profile for the mouse to work
Press Option-Command-P-R until you hear startup sound a second time.	Reset NVRAM		Yes	Yes
Press Option during startup	Start up in Startup Manager, where you can select a Mac OS X volume to start from	Yes	Yes	Yes
Press Eject, F12, or hold the mouse button	Ejects any removable media, such as an optical disc	Yes	Yes	
Press N during startup	Start up from a compatible network server (NetBoot)	Yes	Yes	Yes
Press T during startup	Start up in Target Disk mode			Yes
Press Shift during startup	Start up in Safe Boot mode and temporarily disable login items	Yes	Yes	Known issue with LION to boot to safe mode. "Safe Mode" in red does not appear for Lion
Press Command-V during startup	Start up in Verbose mode.admin	Yes	Yes	Yes
Press Command-S during startup	Start up in Single-User mode	Yes	Yes	Yes
Press Option-N during startup	Start from a NetBoot server using the default boot image	Yes	Yes	Yes
Press Command-R	Start from Lion	N/A	N/A	Yes

Keystroke	Description	Virtual Media CIM	Dual Virtual Media CIM	Mac Lion Server HDMI CIM
during startup	Recovery1			

Using a Windows Keyboard to Access Mac Targets

A Windows® keyboard can be used to access a Mac® connected to a KX III. Windows keys are then used to emulate the special Mac keys. This is the same as connecting a Windows keyboard directly to the Mac.

TCP and UDP Ports Used

▶ Listening TCP Ports:

- * 80: http access (configurable)
- * 443: https access (configurable)
- * 5000: CC-SG and KXUS access (configurable)
- * 22: SSH access (if enabled, configurable)

▶ Listening UDP Ports:

- * 162: SNMP access (if SNMP Agent is enabled)
- * 5001: CC_SG event notification (if under CC-SG management)

▶ TCP Ports Outgoing:

- * 389: LDAP authentication (if LDAP is enabled, configurable)
- * 636: LDAPS/StartTLS (if LDAPS/StartTLS is enabled, configurable)
- * 25: SMTP (email) (if enabled)
- * 445: SMB (Windows File System) access (Remote ISO image access).

▶ UDP Ports Outgoing:

- * 514: Syslog (if enabled, configurable)
- * 5001: CC_SG event notification (if under CC-SG management, configurable)
- * 1812: RADIUS authentication (if enabled, configurable)
- * 1813: RADIUS authentication (if enabled, configurable)

Software

Supported Operating Systems, Browsers and Java Versions

Operating Systems	Browsers	Java
Windows 10	Windows Edge Internet Explorer® 11 Chrome 46 Firefox® 41	Java 1.7 or later for VKC Java 1.8.0_40 or later for VKCs
Windows 7® Home Premium SP1 64-bit	Internet Explorer® 10, 11 Firefox® 29.0.1, 30, 40 Chrome® 35, 45 Safari® 7.0.3, 7.0.5 Edge	Java 1.7 or later for VKC Java 1.8.0_40 or later for VKCs
Windows 7 Ultimate SP1 64-bit		
Windows 7 Ultimate 32-bit		
Windows 8® 64-bit		
Windows XP® Home Edition with SP 3		
Windows Server 2012® Standard 64-bit		
Windows Server 2008 ®		
Windows Server 2003®		
openSUSE® 11.4 Celadon (x86_64)	Firefox 16.0.2	
openSUSE® 13.2	Firefox 33	
Fedora® 18 (Spherical Cow)	Firefox 24	
Fedora ® 22	Firefox 38	
RHEL® 6.4	Firefox 21	
Mac® OS X Mountain Lion® 10.7.5	Firefox 25 Safari 6.0.5	
Mac OS X Mountain Lion 10.8.5 *	Firefox 25 Safari 6.1.1	
Mac 10.10.4	Safari 9.0.1 Chrome 45	
Mac 10.10.5	Safari 9.0.1 Chrome 46	
Solaris® 10 64-bit	Firefox 3.6.23	

**Note: Upon upgrading from OS X 10.8.2 to OS X 10.8.3, Safari® may block Java™.*

JRE Requirements and Browser Considerations for Mac

Java Runtime Environment Requirements for Mac

Install Java Runtime Environment 8 (JRE)® on PCs and Macs® when using the Virtual KVM Client (VKC) to access target devices via KX III.

This ensures in order to provide high performance, KVM-over-IP video processing when remotely accessing target devices/PCs/Macs.

The latest version of JRE for Mac can be downloaded from the Oracle Support website.

Browser Considerations for Mac

Java may be disabled by default in certain browsers. Enable Java and accept all security warnings in order to use KX III.

Certain versions of Safari® block Java for security reasons. Since Java is required to use KX III, Raritan recommends you use Firefox® instead.

Additionally, you may be required to navigate through a number of messages. Select 'Do Not Block' if these messages are displayed.

Virtual KVM Client (VKC), VKCS, and Active KVM Client (AKC) Requirements

Microsoft .NET® 4.0 (or later) is required to use KX III with the Microsoft Windows®-based Active KVM Client (AKC).

Java™ 1.7 is required to use the Java-based . Java 1.8.0_40 is required to use the VKCS.

Java 1.8.0_40 or later is required for VKCS, the standalone VKC client used on Chrome.

KX III checks your current Java version and prompts you to update it if it is not compatible.

VKC can only be launched from a 32-bit browser, or 64-bit browser.

Following are the Java 32-bit and 64-bit Windows operating system requirements.

Mode	Operating system	Browser
Windows x64 32-bit mode	Windows XP®	- Internet Explorer® 7.0, 9.0, 10.0 or 11.0 - Firefox® 1.06 - 4 or later
	Windows Server 2003®	- Internet Explorer 6.0 SP1++, 9.0, 10.0 or 11.0 - Firefox 1.06 - 3
	Windows Vista®	Internet Explorer 9.0, 10.0 or 11.0
	Windows 7®	- Internet Explorer 9.0, 10.0 or 11.0 - Firefox 1.06 - 4 or later
Windows x64 64-bit mode	Windows XP	64bit OS, 32bit browsers: - Internet Explorer 6.0 SP1+, 7.0 or 8.0 - Firefox 1.06 - 4 or later 64bit mode, 64bit browsers: - Internet Explorer 7.0, 8.0, 9.0, 10.0 or 11.0
	Windows XP Professional®	
	Windows XP Tablet®	
	Windows Vista	
	Windows Server 2003	
	Windows Server 2008	
	Windows 7	

Note that a JRE™ plug-in is available for the Windows® 32-bit and 64-bit operating systems.

See *Java Runtime Environment (JRE) Notes* (on page 444) for additional information.

Multi-Language Keyboard JRE Requirement

In order for multi-language keyboards to work in the KX III and Virtual KVM Client (VKC), install the multi-language version of JRE™.

Events Captured in the Audit Log and Syslog

Following is a list and description of the events that are captured by the KX III audit log and syslog:

- Access Login - A user has logged in to the KX III
- Access Logout - A user has logged out of the KX III
- Active USB Profile - The USB profile is active
- CIM Connected - A CIM was connected
- CIM Disconnected - A CIM was disconnected
- Connection Lost - The connection to the target was lost
- Disconnected User - A user was disconnected from a port
- Duplicate CIM Serial - A CIM has same serial number with other CIM.
- End CC Control - CC-SG management ended
- Login Failed - User login failed
- Password Changed - Password change occurred
- Port Connect - Port was connected
- Port Disconnect - Port was disconnected
- Port Status Change - Change in the port status
- Scan Started - A target scan was started
- Scan Stopped - A target scan was stopped
- Session Timeout - A session timeout occurred
- USB Profile Set Modify Failed - Failed to change USB Profile Set.
- USB Profile Set Modified - USB Profile Set was modified.
- USB Net Present - A broadband modem is plugged in.
- USB Net Absent - A broadband modem is unplugged.
- VM Image Connected - A VM image was connected
- VM Image Disconnected - A VM image was disconnected

BSMI Certification

設備名稱：KVM-over-IP 數位切換器		型號（型式）：DKX3系列(系列型號參見次頁)				
Equipment name		Type designation (Type)				
單元 Unit	限用物質及其化學符號					
	Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr ⁺⁶)	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
電路板	—	○	○	○	○	○
電源供應器	—	○	○	○	○	○
機殼	○	○	○	○	○	○
面板	○	○	○	○	○	○
其他配件	○	○	○	○	○	○
備考1. “超出0.1 wt %”及“超出0.01 wt %”係指限用物質之百分比含量超出百分比含量基準值。 Note 1 : “Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.						
備考2. “○”係指該項限用物質之百分比含量未超出百分比含量基準值。 Note 2 : “○” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.						
備考3. “—”係指該項限用物質為排除項目。 Note 3 : The “—” indicates that the restricted substance corresponds to the exemption.						

系列型號:

DKX3-108	DKX3-116	DKX3-132
DKX3-216	DKX3-232	DKX3-416
DKX3-432	DKX3-464	DKX3-808
DKX3-832	DKX3-864	

Appendix E Informational Notes

In This Chapter

Overview	444
Java Runtime Environment (JRE) Notes.....	444
IPv6 Support Notes	446
Dual Stack Login Performance Issues	447
CIM Notes	447
Virtual Media Notes.....	449
USB Port and Profile Notes	452
Video Mode and Resolution Notes	454
Keyboard Notes.....	456
Mouse Notes.....	459
Audio	460
Smart Card Notes	461
CC-SG Notes.....	461
Browser Notes	461

Overview

This section includes important notes on KX III usage. Future updates will be documented and available online through the Help link in the KX III Remote Console interface.

Note: Some topics in this section reference other multiple Raritan appliances because various appliances are impacted by the information.

Java Runtime Environment (JRE) Notes

Disable Java Caching and Clear the Java Cache

It is highly recommended that you disable Java caching in Microsoft Windows®, and clear the Java™ cache.

► **To disable Java caching and clear the cache:**

1. From the Windows Start menu, click Control Panel.
2. Double-click on the Java icon to launch it. The Java Control Panel dialog appears.
3. To disable Java caching:
 - a. From the General tab, click the Settings button. The Temporary Files Settings dialog appears.

- b. Click the View Applets button. The Java Applet Cache Viewer opens.
 - c. Deselect the Enable Caching checkbox if it is already checked.
 - d. Click OK.
4. To clear the Java cache:
- a. From the Temporary Files Settings dialog, click the Delete Files button. The Delete Temporary Files dialog appears.
 - b. Select the temporary files that you want to delete.
 - c. Click OK.

Java Not Loading Properly on Mac

If you are using a Mac® and see the following message when connecting to a device from the KX III Port Access Table, Java™ is not loaded properly:

"Error while getting the list of open targets, please try again in a few seconds".

If this occurs, check your Java installation from this website:

<http://www.java.com/en/download/testjava.jsp>

<http://www.java.com/en/download/testjava.jsp>

If your Java applet is inactive, it can be enabled from this page. If it is not installed correctly, a message lets you know and you can then reinstall Java.

IPv6 Support Notes

Operating System IPv6 Support Notes

Java

Java™ 1.7 supports IPv6 for the following:

- Solaris™ 10 (and later)
- Linux® kernel 2.1.2 (and later)/RedHat 6.1 (and later)
- Solaris 10 (and later)
- Windows XP® SP1 and Windows 2003®, Windows Vista®, Windows 7®, Windows 8®, and Windows 10®, operating systems

Linux

- It is recommended that Linux kernel 2.4.0 or higher is used when using IPv6.
- An IPv6-enabled kernel will need to be installed or the kernel will need to be rebuilt with IPv6 options enabled.
- Several network utilities will also need to be installed for Linux when using IPv6. For detailed information, refer to <http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html>

Windows

- Windows XP and Windows 2003 users will need to install the Microsoft IPv6 service pack to enable IPv6.
- For AKC with IPv6 on Windows XP, add the executable kxgui.exe to your firewall exception list. View your log file on the client to identify the full path for the location of the file kxgui.exe.

Samba

- IPv6 is not supported for use with virtual media when using Samba.

AKC Download Server Certification Validation IPv6 Support Notes

If you are connecting to a KX III standalone device and support for AKC download server certificate validation is enabled, the valid IPv6 format to generate the certificate is either:

- CN =[fd07:02fa:6cff:2500:020d:5dff:fe00:01c0] when there is a leading 0
- or
- CN =[fd07:02fa:6cff:2500:020d:5dff:0000:01c0] when there is no zero compression

Dual Stack Login Performance Issues

If you are using the KX III in a dual stack configuration, it is important you configured the domain system (DNS) correctly in the KX III in order to avoid delays when logging in.

See *Tips for Adding a Web Browser Interface* (on page 128) for information on configuring your DNS in KX III.

CIM Notes

Windows 3-Button Mouse on Linux Targets

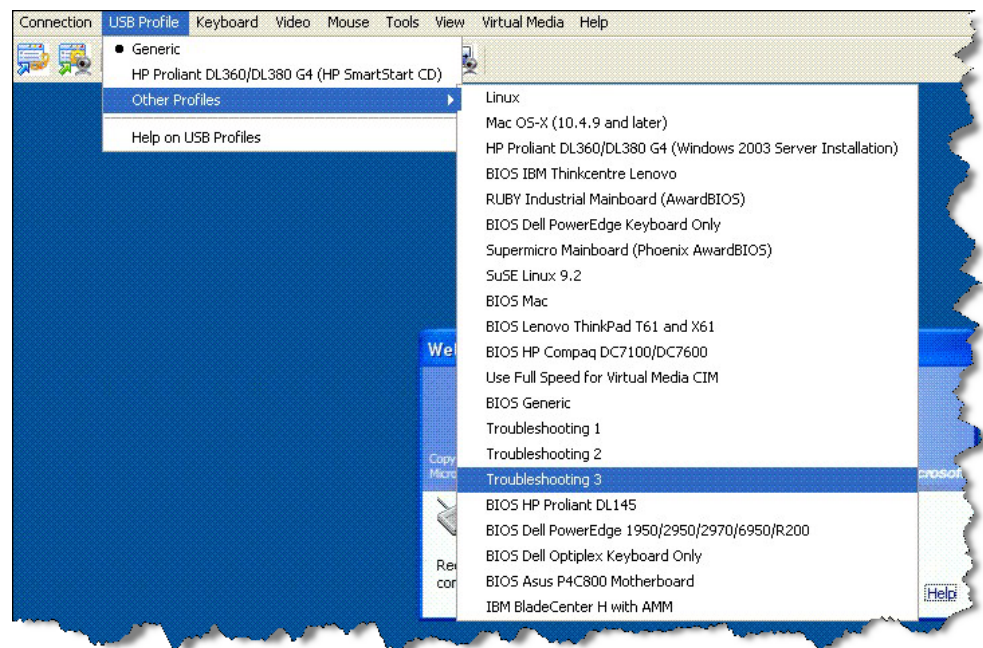
When using a 3-button mouse on a Windows® client connecting to a Linux® target, the left mouse button may get mapped to the center button of the Windows client 3-button mouse.

Windows 2000 Composite USB Device Behavior for Virtual Media

The Windows 2000® operating system does not support USB composite devices, like Raritan's D2CIM-VUSB, in the same manner as non-composite USB devices.

As a result, the "Safely Remove Hardware" system tray icon does not appear for drives mapped by the D2CIM-VUSB and a warning message may appear when disconnecting the device. Raritan has not observed any problems or issues from this message, however.

Raritan's US engineering department has developed a configuration which supports the "Safely Remove Hardware" icon and avoids this Windows message. This configuration requires the use of the D2CIM-DVUSB virtual media adapter and the Troubleshooting 3 USB Profile that configures the D2CIM-DVUSB as a non-composite USB device supporting a single virtual media connection. Raritan has successfully tested this configuration in the US and Japan.



Target Video Picture Not Centered (Mouse Out of Synch)

At certain resolutions when using an HDMI or DVI CIM with the KX III:

- The video display may not be centered properly - black rectangles can be seen at the edges of the screen
- The mouse on the target may appear to be slightly out of synch

If either or both of these occur, you may be able to correct this by adjusting the display scaling options from the target computer's video controller software.

For example, if your target computer uses the Catalyst Control Center video controller, adjust the Underscan/Overscan setting as needed.

Powerstrip is not detected

When the PowerCIM-PDU is disconnected physically from the KX3, the PDU is still listed in the PowerStrip Device drop-down list with a "Powerstrip is not detected, please check!" message that does not disappear.

► To solve:

In the port configuration page for the port, click Reset To Default.

Virtual Media Notes

Cannot Connect to Drives from Linux Clients

If you cannot connect to a virtual media drive on a target server when you connect from a client running Linux® Fedora™ 18 with Java™ 1.7 (update 45 and later), disable SELinux in Fedora 18 on the client to resolve the problem.

Cannot Write To/From a File from a Mac Client

If you are connecting to the KX III from a Mac® 10.8.5 client running Safari with Java™ 1.7 and cannot write to/from a file on a KX2 or KX3 target server or access virtual media, do the following to correct this:

1. In Safari, select Preferences.
2. Under the Security tab, select Manage Website Settings.
3. Click on "Website for KX2 or KX3".
4. Select "Run in unsafe mode" from the drop-down.

Note: In Safari 10.0, "Run in safe mode" is now hidden as an option for Plugin-Settings. Hold the Mac Option/Alt key while clicking on the site to list the option.

If running MacOS Sierra 10.12, Java version must be 1.8.0.121 or higher.

- 5. Restart Safari.

Virtual Media via VKC and AKC in a Windows Environment

Windows XP® operating system administrator and standard user privileges vary from those of the Windows Vista® operating system and the Windows 7® operating system.

When enabled in Vista or Windows 7, User Access Control (UAC) provides the lowest level of rights and privileges a user needs for an application. For example, a Run as Administrator option is provided for Internet Explorer® for Administrator level tasks; otherwise these are not accessible even though the user has an Administrator login.

Both features affect the types of virtual media that can be accessed in VKC, VKCS, and AKC. See your Microsoft® help for additional information on these features and how to use them.

Following is a list virtual media types users can access via VKC and AKC when running in a Windows environment. The features are broken down by client and the virtual media features that are accessible to each Windows user role.

Windows XP

If you are running VKC and AKC in a Windows XP environment, users must have Administrator privileges to access any virtual media type other than CD-ROM connections, ISOs and ISO images.

Windows Vista and Windows 7

If you are running VKC and AKC in a Windows Vista or Windows 7 environment and UAC is enabled, the following virtual media types can be accessed depending on the user's Windows role:

Client	Administrator	Standard User
AKC and VKC	Access to: - Fixed drives and fixed drive partitions - Removable drives - CD/DVD drives - ISO images - Remote ISO images	Access to: - Removable drives - CD/DVD drives - ISO images - Remote ISO images

Virtual Media Support on Windows 10, Windows 7, Windows 2008 and Windows XP Targets

Virtual media is not supported on a Windows 10, Windows 7, Windows 2008 or Windows XP target server when connecting via VKC and AKC from Windows 10, Windows 2008, Windows 2012.

Virtual Media Not Refreshed After Files Added

After a virtual media drive has been mounted, if you add a file(s) to that drive, those files may not be immediately visible on the target server. Disconnect and then reconnect the virtual media connection.

Virtual Media Linux Drive Listed Twice

For KX III, users who are logged in to Linux™ clients as root users, the drives are listed twice in the Local Drive drop-down.

For example, you will see eg /dev/sdc and eg /dev/sdc1 where the first drive is the boot sector and the second drive is the first partition on the disk.

Accessing Virtual Media on a Windows 2000

A virtual media local drive cannot be accessed on a Windows 2000® server using a D2CIM-VUSB.

Disconnecting Mac and Linux Virtual Media USB Drives

In a Linux® or Mac® environment:

- For Linux users, if there is /dev/sdb and /dev/sdb1, the client only uses /dev/sdb1 and advertise it as removable disk
- /dev/sdb is not available for the user.
- For Linux users, if there is /dev/sdb but no /dev/sdb1, /dev/sdb is used as a removable device
- For Mac users, /dev/disk1 and /dev/disk1s1 is used

Target BIOS Boot Time with Virtual Media

The BIOS for certain targets may take longer to boot if media is mounted virtually at the target.

► To shorten the boot time:

1. Close the Virtual KVM Client to completely release the virtual media drives.
2. Restart the target.

Virtual Media Connection Failures Using High Speed for Virtual Media Connections

Under certain circumstances it may be necessary to select the "Use Full Speed for Virtual Media CIM" when a target has problems with "High Speed USB" connections or when the target is experiencing USB protocol errors caused by signal degradation due to additional connectors and cables (for example, a connection to a blade server via a dongle).

USB Port and Profile Notes

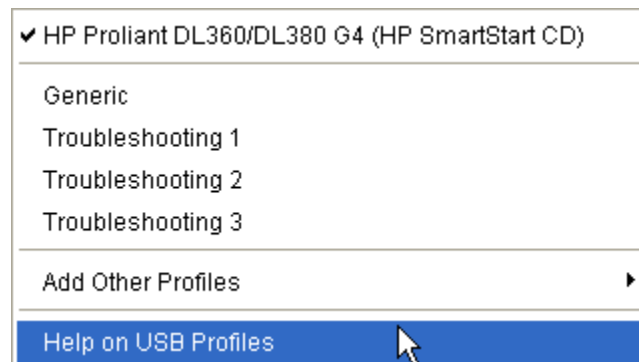
VM-CIMs and DL360 USB Ports

HP® DL360 servers have one USB port on the back of the device and another on the front of the device. With the DL360, both ports cannot be used at the same time. Therefore, a dual VM-CIM cannot be used on DL360 servers.

However, as a workaround, a USB2 hub can be attached to the USB port on the back of the device and a dual VM-CIM can be attached to the hub.

Help Choosing USB Profiles

When you are connected to a KVM target server via the Virtual KVM Client (VKC), you can view information about USB profiles via the Help on USB Profiles command on the USB Profile menu.



USB profile help appears in the USB Profile Help window. For detailed information about specific USB profiles, see Available USB Profiles.

Raritan provides a standard selection of USB configuration profiles for a wide range of operating system and BIOS level server implementations. These are intended to provide an optimal match between remote USB device and target server configurations.

The 'Generic' profile meets the needs of most commonly deployed target server configurations.

Additional profiles are made available to meet the specific needs of other commonly deployed server configurations (for example, Linux®, Mac OS X®).

There are also a number of profiles (designated by platform name and BIOS revision) that have been tailored to enhance the virtual media function compatibility with the target server, for example, when operating at the BIOS level.

'Add Other Profiles' provides access to other profiles available on the system. Profiles selected from this list will be added to the USB Profile Menu. This includes a set of 'trouble-shooting' profiles intended to help identify configuration limitations.

The USB Profile Menu selections are configurable via the Console Device Settings > Port Configuration page.

Should none of the standard USB profiles provided by Raritan meet your target server requirements, Raritan Technical Support can work with you to arrive at a solution tailored for that target. Raritan recommends that you do the following:

1. Check the most recent release notes on the Raritan website (www.raritan.com) on the Firmware Upgrade page to see if a solution is already available for your configuration.
2. If not, please provide the following information when contacting Raritan Technical Support:
 - a. Target server information, manufacturer, model, BIOS, manufacturer, and version.
 - b. The intended use (e.g. redirecting an image to reload a server's operating system from CD).

Changing a USB Profile when Using a Smart Card Reader

There may be certain circumstances under which you will need to change the USB profile for a target server. For example, you may need to change the connection speed to "Use Full Speed for Virtual Media CIM" when the target has problems with the "High Speed USB" connection speed.

When a profile is changed, you may receive a New Hardware Detected message and be required to log in to the target with administrative privileges to reinstall the USB driver. This is only likely to occur the first few times the target sees the new settings for the USB device. Afterward, the target will select the driver correctly.

Video Mode and Resolution Notes

Video Image Appears Dark when Using a Mac

If you are using a Mac® with an HDMI video port and the video seems too dark, enable DVI Compatibility Mode on the CIM to help resolve the issue. See *Configuring CIM Ports* (on page 102)

Video Shrinks after Adjusting Target Clock

On HP® ProLiant® DL380p G8 target servers, certain resolutions cause the target video to shrink. This is caused when the server's clock attempts to auto-adjust and detects the wrong active line length.

Depending on the resolution the target is set to, this occurs when connecting to the HP target from the KX III Remote Console or Local Port, or both the Remote Console and Local Port. This issue was detected at the following resolutions:

Target resolution	Issue seen on Local Port	Issue seen from Remote Console
1440x900@60Hz	Yes	Yes
1400x1050@60Hz	No	Yes
1152x864@60Hz	No	Yes

Black Stripe/Bar(s) Displayed on the Local Port

Certain servers and video resolutions may display on the local port with small black bars at the edge of the screen.

If this occurs:

1. Try a different resolution, or
2. If using a digital CIM, then change the Display Native Resolution on the Port Configuration page to another resolution, or
3. If using the HDMI CIM, use the DVI Compatibility Mode.

Contact Raritan Technical Support for additional assistance.

Sun Composite Synch Video

Sun™ composite synch video is not supported.

SUSE/VESA Video Modes

The SuSE X.org configuration tool SaX2 generates video modes using modeline entries in the X.org configuration file. These video modes do not correspond exactly with VESA video mode timing (even when a VESA monitor is selected). The KX III, on the other hand, relies on exact VESA mode timing for proper synchronization. This disparity can result in black borders, missing sections of the picture, and noise.

► **To configure the SUSE video display:**

1. The generated configuration file `/etc/X11/xorg.conf` includes a Monitor section with an option named `UseModes`. For example, `UseModes "Modes[0]"`
2. Either comment out this line (using `#`) or delete it completely.
3. Restart the X server.

With this change, the internal video mode timing from the X server is used and corresponds exactly with the VESA video mode timing, resulting in the proper video display on the KX III.

Keyboard Notes

French Keyboard

Caret Symbol (Linux Clients Only)

The Virtual KVM Client (VKC) do not process the key combination of Alt Gr + 9 as the caret symbol (^) when using French keyboards with Linux® clients.

► **To obtain the caret symbol:**

From a French keyboard, press the ^ key (to the right of the P key), then immediately press the space bar.

Alternatively, create a macro consisting of the following commands:

1. Press Right Alt
2. Press 9.
3. Release 9.
4. Release Right Alt.

Note: These procedures do not apply to the circumflex accent (above vowels). In all cases, the ^ key (to the right of the P key) works on French keyboards to create the circumflex accent when used in combination with another character.

Accent Symbol (Windows XP Operating System Clients Only)

From the Virtual KVM Client (VKC), the key combination of Alt Gr + 7 results in the accented character displaying twice when using French keyboards with Windows XP® clients.

Note: This does not occur with Linux® clients.

Numeric Keypad

From the Virtual KVM Client (VKC), the numeric keypad symbols display as follows when using a French keyboard:

Numeric keypad symbol	Displays as
/	;
.	;

Tilde Symbol

From the Virtual KVM Client (VNC), the key combination of Alt Gr + 2 does not produce the tilde (~) symbol when using a French keyboard.

► **To obtain the tilde symbol:**

Create a macro consisting of the following commands:

- Press right Alt
- Press 2
- Release 2
- Release right Alt

Keyboard Language Preference (Fedora Linux Clients)

Because the Sun™ JRE™ on Linux® has problems generating the correct KeyEvents for foreign-language keyboards configured using System Preferences, Raritan recommends that you configure foreign keyboards using the methods described in the following table.

Language	Configuration method
US Intl	Default
UK	System Settings (Control Center)
French	Keyboard Indicator
German	Keyboard Indicator
Hungarian	System Settings (Control Center)
Spanish	System Settings (Control Center)
Swiss-German	System Settings (Control Center)
Norwegian	Keyboard Indicator
Swedish	Keyboard Indicator
Danish	Keyboard Indicator
Japanese	System Settings (Control Center)
Korean	System Settings (Control Center)
Slovenian	System Settings (Control Center)
Italian	System Settings (Control Center)
Portuguese	System Settings (Control Center)

Note: The Keyboard Indicator should be used on Linux systems using Gnome as a desktop environment.

When using a Hungarian keyboard from a Linux client, the Latin letter U with Double Acute and the Latin letter O with Double Acute work only with JRE 1.6 (and later).

There are several methods that can be used to set the keyboard language preference on Fedora® Linux clients. The following method must be used in order for the keys to be mapped correctly from the Virtual KVM Client (VKC).

► **To set the keyboard language using System Settings:**

1. From the toolbar, choose System > Preferences > Keyboard.
2. Open the Layouts tab.
3. Add or select the appropriate language.
4. Click Close.

► **To set the keyboard language using the Keyboard Indicator:**

1. Right-click the Task Bar and choose Add to Panel.
2. In the Add to Panel dialog, right-click the Keyboard Indicator and from the menu choose Open Keyboard Preferences.
3. In the Keyboard Preferences dialog, click the Layouts tab.
4. Add and remove languages as necessary.

Macros Not Saving on Linux Targets

If you receive the following error message when you create and then save a macro on a target server running Linux® Fedora™ 18 with Java™ 1.7.0 (update 45 and later), disable SELinux in Fedora 18 on the target server to resolve the problem.

"An error occurred attempting to write the new keyboard macros. Macro was not added"

Mac Keyboard Keys Not Supported for Remote Access

When a Mac® is used as the client, the following keys on the Mac® keyboard are not captured by the Java™ Runtime Environment (JRE™):

- F9
- F10
- F11
- F14
- F15
- Volume Up
- Volume Down
- Mute
- Eject

As a result, the Virtual KVM Client (VKC) are unable to process these keys from a Mac client's keyboard.

Mouse Notes

Mouse Pointer Synchronization (Fedora)

When connected in dual mouse mode to a target device running Fedora® 7, if the target and local mouse pointers lose synchronization, changing the mouse mode from or to Intelligent or Standard may improve synchronization.

Single mouse mode may also provide for better control.

► **To resynchronize the mouse cursors:**

- Use the Synchronize Mouse option from the Virtual KVM Client (VKC).

Single Mouse Mode when Connecting to a Target Under CC-SG Control

When using Firefox® to connect to a KX III target under CC-SG control using DCIM-PS2 or DCIM-USBG2, if you change to Single Mouse Mode in the Virtual KVM Client (VKC), the VKC window will no longer be the focus window and the mouse will not respond.

If this occurs, left click on the mouse or press Alt+Tab to return the focus to the VKC window.

Mouse Sync Issues in Mac OS 10

In Mac OS 10, if mouse sync is an issue at some resolutions, use USB profile "General" and Absolute mouse mode.

Audio

Audio Playback and Capture Issues

Features that May Interrupt an Audio Connection

If you use any of the following features while connected to an audio device, your audio connection may be interrupted. Raritan recommends you do not use these features if you are connected to an audio device:

- Video Auto-Sense
- Extensive use of the local port
- Adding users

Issues when Using a Capture Device and Playback Device Simultaneously on a Target

On some targets, the simultaneous connection of capture devices and playback devices may not work due to the USB hub controller and how it manages the USB ports. Consider selecting an audio format that requires less bandwidth.

If this does not resolve the issue, connect the D2CIM-DVUSB CIM's keyboard and mouse connector to a different port on the target. If this does not solve the problem, connect the device to a USB hub and connect the hub to the target.

Audio in a Linux Environment

The following are known issues when using the audio feature in a Linux® environment.

- Linux® users, use the default audio device for playback. Sound may not come through if a non-default sound card is selected.
- SuSE 11 clients require Javas_1_6_0-sun-alsa (ALSA support for java-1_6_0-sun) to be installed via YAST.
- For Logitech® headsets with a built in a mic, only the Mono Capture option is available.
- In order to display the device, if you are running SUSE 11 and an ALSA driver, log out of KX III, then log back in.

Additionally, if you connect and disconnect the audio device a number of times, the device may be listed several times vs. just once as it should.

- Using the audio feature with a Fedora Core® 13 target set to mono 16 bit, 44k may cause considerable interference during playback.

Audio in a Windows Environment

On Windows® 64-bit clients, only one playback device is listed on the Connect Audio panel when accessing the device through the Virtual KVM Client (VKC).

The audio device is the default device, and is listed on the Connect Audio panel as Java Sound Audio Engine.

Smart Card Notes

Virtual KVM Client (VKC) Smart Card Connections to Fedora Servers

If you are using a smart card to connect to a Linux® Fedora® server via Virtual KVM Client (VKC) upgrade the pcsc-lite library to 1.4.102-3 or above.

CC-SG Notes

Virtual KVM Client Version Not Known from CC-SG Proxy Mode

When the Virtual KVM Client (VKC) is launched from CommandCenter Secure Gateway (CC-SG) in proxy mode, the VKC version is unknown.

In the About Raritan Virtual KVM Client dialog, the version is displayed as "Version Unknown".

Moving Between Ports on a Device

If you move a between ports on the same Raritan device and resume management within one minute, CC-SG may display an error message.

If you resume management, the display will be updated.

Browser Notes

Resolving Issues with Firefox Freezing when Using Fedora

If you are accessing Firefox® and are using a Fedora® server, Firefox may freeze when it is opening.

To resolve this issue, install the libnjp2.so Java™ plug-in on the server.

Appendix F Frequently Asked Questions

In This Chapter

General FAQs	462
Remote Access.....	465
Universal Virtual Media	468
Bandwidth and KVM-over-IP Performance	470
IPv6 Networking	474
Servers.....	476
Blade Servers.....	476
Installation.....	478
Local Port - KX IIII	481
Extended Local Port.....	482
Dual Power Supplies.....	483
Intelligent Power Distribution Unit (PDU) Control	483
Ethernet and IP Networking.....	485
Local Port Consolidation, Tiering and Cascading	486
Computer Interface Modules (CIMs)	489
Security	490
Smart Cards and CAC Authentication.....	492
Manageability	493
Documentation and Support.....	495
Miscellaneous	496

General FAQs

Question	Answer
What is Dominion KX III?	Dominion KX III is a third-generation digital KVM (keyboard, video, mouse) switch that enables one, two, four or eight IT administrators to access and control 8, 16, 32 or 64 servers over the network with BIOS-level functionality. Dominion KX III is completely hardware- and OS-independent; users can troubleshoot and reconfigure servers even when servers are down. At the rack, Dominion KX III provides the same functionality, convenience, and space and cost savings as traditional analog KVM switches. However, Dominion KX III also integrates the industry's highest performing KVM-over-IP technology, allowing multiple administrators to access server KVM consoles from any networked workstation as well as from the iPhone® and iPad®.

Question	Answer
How is KX III different from KX II ?	The KX III is the next generation version of the KX II. Featuring a modern hardware design with increased computing power and storage, the KX III provides KVM-over-IP access for IT administration, as well as high performance IP access for broadcast applications. KX III includes virtually all KX II features with the following advancements: The KX III's new video processing engine supports a broad range of applications from traditional computer applications to the most dynamic broadcast applications requiring 30 frames-per-second 1920x1080 video, 24 bit color, digital audio, dual monitors and DVI, HDMI, DisplayPort and VGA video. With the industry's first DVI-based local port, the KX III's common user interface provides new levels of productivity and performance for at-the-rack administration and server access. All KX III models feature a tiering port to connect multiple Dominion KX III switches together and access the attached servers. Up to 1024 servers can be accessed via a consolidated port list. KX III supports all Dominion and Paragon II CIMs supported by KX II.

Question	Answer
How does Dominion KX III differ from remote control software?	When using Dominion KX III remotely, the interface, at first glance, may seem similar to remote control software such as pcAnywhere™, Windows® Terminal Services/Remote Desktop, VNC, etc. However, because Dominion KX III is not a software but a hardware solution, it's much more powerful: Hardware- and OS-independent – Dominion KX III can be used to manage servers running many popular OSs, including Intel®, Sun®, PowerPC running Windows, Linux®, Solaris™, etc. State-independent/Agentless – Dominion KX III does not require the managed server OS to be up and running, nor does it require any special software to be installed on the managed server. Out-of-band – Even if the managed server's own network connection is unavailable, it can still be managed through Dominion KX III. BIOS-level access – Even if the server is hung at boot up, requires booting to safe mode, or requires system BIOS parameters to be altered, Dominion KX III still works flawlessly to enable these configurations to be made.
Can the Dominion KX III be rack mounted?	Yes. The Dominion KX III ships standard with 19" rack mount brackets. It can also be reverse rack mounted so the server ports face forward.
How large is the Dominion KX III?	Dominion KX III is only 1U high (except the KX3-864 and KX3-464, which are 2U), fits in a standard 19" rack mount and is only 11.4" (29 cm) deep. The Dominion KX3-832 and KX3-864 are 13.8" (36 cm) deep.

Remote Access

Question	Answer
How many users can remotely access servers on each Dominion KX III?	Dominion KX III models offer remote connections for up to eight users per user channel to simultaneously access and control a unique target server. For one-channel appliances like the DKX3-116, up to eight remote users can access and control a single target server. For two-channel appliances, like the DKX3-216, up to eight users can access and control the server on channel one and up to another eight users on channel two. For four-channel appliances, up to eight users per channel, for a total of 32 (8 x 4) users, can access and control four servers. Likewise, for the eight-channel appliances, up to eight users can access a single server, up to an overall maximum of 32 users across the eight channels.
Can I remotely access servers from my iPhone or iPad?	Yes. Users can access servers connected to the KX III using their iPhone or iPad. Mobile access is provided through Mobile Access Client, which requires the use of CommandCenter Secure Gateway (CC-SG).
Can two people look at the same server at the same time?	Yes. Actually, up to eight people can access and control any single server at the same time.
Can two people access the same server, one remotely and one from the local port?	Yes. The local port is completely independent of the remote "ports." The local port can access the same server using the PC-Share feature.

Question	Answer															
In order to access Dominion KX III from a client, what hardware, software or network configuration is required?	Because Dominion KX III is completely Web-accessible, it doesn't require customers to install proprietary software on clients used for access. Dominion KX III can be accessed through major Web browsers, including: Internet Explorer® and Firefox®. Dominion KX III can be accessed on Windows®, Linux® and Mac® desktops, via Raritan's Windows Client, and the Java™-based Virtual KVM Client™. Dominion KX III administrators can also perform remote management (set passwords and security, rename servers, change IP address, etc.) using a convenient browser-based interface.															
What is the file size of the applet that's used to access Dominion KX III? How long does it take to retrieve?	The Virtual KVM Client (VKC) applet used to access Dominion KX III is approximately 500KB in size. The following chart describes the time required to retrieve Dominion KX III's applet at different network speeds: <table><tr><td>100Mbps</td><td>Theoretical 100Mbit network speed</td><td>.05 seconds</td></tr><tr><td>60Mbps</td><td>Likely practical 100Mbit network speed</td><td>.08 seconds</td></tr><tr><td>10Mbps</td><td>Theoretical 10Mbit network speed</td><td>.4 seconds</td></tr><tr><td>6Mbps</td><td>Likely practical 10Mbit network speed</td><td>.8 seconds</td></tr><tr><td>512Kbps</td><td>Cable modem download speed (typical)</td><td>8 seconds</td></tr></table>	100Mbps	Theoretical 100Mbit network speed	.05 seconds	60Mbps	Likely practical 100Mbit network speed	.08 seconds	10Mbps	Theoretical 10Mbit network speed	.4 seconds	6Mbps	Likely practical 10Mbit network speed	.8 seconds	512Kbps	Cable modem download speed (typical)	8 seconds
100Mbps	Theoretical 100Mbit network speed	.05 seconds														
60Mbps	Likely practical 100Mbit network speed	.08 seconds														
10Mbps	Theoretical 10Mbit network speed	.4 seconds														
6Mbps	Likely practical 10Mbit network speed	.8 seconds														
512Kbps	Cable modem download speed (typical)	8 seconds														

Question	Answer
Do you have a Windows KVM Client?	Yes. We have a native .NET Windows Client called the Raritan Active KVM Client (AKC). See <i>Active KVM Client (AKC) Help</i> (on page 301)
Do you have a non-Windows KVM Client?	Yes. The Virtual KVM Client (VKC) allows non-Windows users to connect to target servers in the data center. See <i>Virtual KVM Client (VKC) Help</i> (see " <i>Virtual KVM Client (VKC and VKCs) Help</i> " on page 256)
Do your KVM Clients have multi-language support?	Yes. The Dominion KX III's remote HTML User Interface and the KVM Clients support the Japanese, Simplified Chinese and Traditional Chinese languages. This is available stand-alone as well as through CC-SG.
Do your KVM Clients support dual LCD monitors?	Yes. For customers wishing to enhance their productivity by using multiple LCD monitors on their desktops, the Dominion KX III can launch KVM sessions to multiple monitors, either in full screen or standard modes.
Do you support servers with dual video cards?	Yes, dual video cards are supported with an extended desktop configuration available to the remote user.
How do I access servers connected to Dominion KX III if the network ever becomes unavailable?	You can access servers at the rack or via modem. Dominion KX III offers a dedicated modem port for attaching an external modem.

Universal Virtual Media

Question	Answer
Which Dominion KX III models support virtual media?	All Dominion KX III models support virtual media. It is available stand-alone and through CommandCenter® Secure Gateway, Raritan's centralized management appliance.
Which types of virtual media does the Dominion KX III support?	Dominion KX III supports the following types of media: internal and USB-connected CD/DVD drives, USB mass storage devices, PC hard drives and ISO images.

Question	Answer
What is required for virtual media?	A Dominion KX III virtual media CIM is required. There are two VGA-based CIMs: a D2CIM-VUSB or D2CIM-DVUSB. The D2CIM-VUSB has a single USB connector and is for customers who will use virtual media at the OS level. The D2CIM-DVUSB has dual USB connectors and should be purchased by customers who wish to utilize virtual media at the BIOS level. The D2CIM-DVUSB is also required for smart card authentication, tiering/cascading and digital audio. Both support virtual media sessions to target servers supporting the USB 2.0 interface. Available in economical 32 and 64 quantity CIM packages, these CIMs support Absolute Mouse Synchronization™ as well as remote firmware updates. Our CIMs have traditionally supported analog VGA video. Three new dual virtual media CIMs support digital video formats, including DVI, HDMI and DisplayPort. These are the D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI and D2CIM-DVUSB-DP.
Is virtual media secure?	Yes. Virtual media sessions are secured using 256-bit AES or 128-bit AES encryption.
Does virtual media really support audio?	Yes. Audio playback and recording to a server connected to the Dominion KX III is supported. You can listen to sounds and audio playing on a remote server in the data center using the speakers connected to your desktop PC or laptop. You can also record on the remote server using a microphone connected to your PC or laptop. A digital CIM or D2CIM-DVUSB dual virtual media CIM is required.
What is a USB profile?	Certain servers require a specifically configured USB interface for USB-based services such as virtual media. The USB profile tailors the KX III's USB interface to the server to accommodate these server-specific characteristics.

Question	Answer
Why would I use a USB profile?	USB profiles are most often required at the BIOS level where there may not be full support for the USB specification when accessing virtual media drives. However, profiles are sometimes used at the OS level, for example, for mouse synchronization for Mac and Linux servers.
How is a USB profile used?	Individual ports or groups of ports can be configured by the administrator to use a specific USB profile in the KX III's port configuration page. A USB profile can also be selected in the KX III Client when required. See the user guide for more information.
Do I always need to set a USB profile when I use virtual media?	No. In many cases, the default USB profile is sufficient when using virtual media at the OS level or operating at the BIOS level without accessing virtual media.
What profiles are available? Where can I find more information?	Consult the user guide for the available profiles and for more information.

Bandwidth and KVM-over-IP Performance

Question	Answer
How is bandwidth used in KVM-over-IP systems?	Dominion KX III offers totally new video processing that provides flexible, high performance video, efficient use of bandwidth and anytime/anywhere access via LAN, WAN or Internet. The Dominion KX III digitizes, compresses and encrypts the keyboard, video and mouse signals from the target server and transmits IP packets over the IP network to the remote client to create the remote session to the user. The KX III provides an at-the-rack experience based on its industry-leading video processing algorithms. Screen changes, i.e., video accounts for the majority of the bandwidth used – and keyboard and mouse activity are significantly less. It is important to note that bandwidth is only used when the user is active. The amount of bandwidth used is based on the amount of change to the server's video display screen. If there are no changes to the video – the user is not interacting with the server – there is generally little to no bandwidth used. If the user moves the mouse or types a character, then there is a small amount of bandwidth used. If the display is running a complex screen saver or playing a video, then there can be a larger amount of bandwidth used.
How does bandwidth affect KVM-over-IP performance?	In general, there is a trade-off between bandwidth and performance. The more bandwidth available, the better performance can be. In limited bandwidth environments, performance can degrade. The Dominion KX III has been optimized to provide strong performance in a wide variety of environments.

Question	Answer
What factors affect bandwidth?	There are many factors that determine how much bandwidth will be used. The primary factor, noted above, is the amount of change in the target server's video display. This is dependent on the user's task and actions. Other factors include the server's video resolution, networking speed and characteristics, the KVM Client Connection Properties, client PC resources and video card noise.
How much bandwidth does KX III use for common tasks?	Bandwidth primarily depends on the user's task and actions. The more the server's video screen changes, the more bandwidth is utilized.

Question	Answer
How do I optimize performance and bandwidth?	KX III provides a variety of settings in our remote clients for the user to optimize bandwidth and performance. The default settings will provide an at-the-rack level of performance in standard LAN/WAN environments with economical use of bandwidth. Optimize For. Use this setting to configure the video engine for standard IT/computer applications or for video/broadcast applications. Compression. Move the slider to the left for the highest possible video quality and to the right for the least amount of bandwidth. Noise Filter. In most cases, the default setting will work best, however you can move to the left for more responsive video and to the right for lower bandwidth. Other tips to decrease bandwidth include: ▪ Use a solid desktop background instead of a complex image ▪ Disable screensavers ▪ Use a lower video resolution on the target server ▪ Uncheck the "Show window contents while dragging" option in Windows ▪ Use simple images, themes and desktops (e.g., Windows Classic)
I want to connect over the Internet. What type of performance should I expect?	It depends on the bandwidth and latency of the Internet connection between your remote client and the KX III. With a cable modem or high speed DSL connection, your performance can be very similar to a LAN/WAN connection. For lower speed links, use the suggestions above to improve performance.

Question	Answer
I have a high bandwidth environment. How can I optimize performance?	The default settings will work well. You can move the Connection Properties settings to the left for increased video performance.
What is the maximum remote (over IP) video resolution supported?	The Dominion KX III is the first and only KVM-over-IP switch to support full high definition (HD) remote video resolution – 1920x1080 at frame rates up to 30 frames per second with digital audio. In addition, popular widescreen formats are supported, including 1600x1200, 1680x1050 and 1440x900, so remote users can work with today's higher resolution monitors.
How much bandwidth is used for audio?	It depends on the type of audio format used, but to listen to CD quality audio, approximately 1.5 Mbps is used.
What about servers with DVI ports?	Servers with DVI ports that support DVI-A (analog) and DVI-I (integrated analog and digital) can use Raritan's ADVI-VGA inexpensive, passive adapter to convert the server's DVI port to a VGA plug that can be connected to a KX III CIM's VGA plug. Servers with DVI ports that support DVI-I or DVI-D (digital) can use the new D2CIM-DVUSB-DVI CIM.

IPv6 Networking

Question	Answer
What is IPv6?	IPv6 is the acronym for Internet Protocol Version 6. IPv6 is the "next generation" IP protocol which will replace the current IP Version 4 (IPv4) protocol. IPv6 addresses a number of problems in IPv4, such as the limited number of IPv4 addresses. It also improves IPv4 in areas such as routing and network auto-configuration. IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years. IPv6 treats one of the largest headaches of an IP network from the administrator's point of view – configuring and maintaining an IP network.
Why does KX III support IPv6 networking?	U.S. government agencies and the Department of Defense are now mandated to purchase IPv6-compatible products. In addition, many enterprises and foreign countries, such as China, will be transitioning to IPv6 over the next several years.
What is "dual stack" and why is it required?	Dual stack is the ability to simultaneously support IPv4 and IPv6 protocols. Given the gradual transition from IPv4 to IPv6, dual stack is a fundamental requirement for IPv6 support.
How do I enable IPv6 on the KX III?	Use the "Network Settings" page, available from the "Device Settings" tab. Enable IPv6 addressing and choose manual or auto-configuration. Consult the user guide for more information.
What if I have an external server with an IPv6 address that I want to use with my KX III?	The KX III can access external servers via their IPv6 addresses, for example, an SNMP manager, syslog server or LDAP server. Using the KX III's dual-stack architecture, these external servers can be accessed via: (1) an IPv4 address, (2) IPv6 address or (3) hostname. So, the KX III supports the mixed IPv4/IPv6 environment many customers will have.
What if my network doesn't support IPv6?	The KX III's default networking is set at the factory for IPv4 only. When you are ready to use IPv6, then follow the above instructions to enable IPv4/IPv6 dual-stack operation.

Question	Answer
Where can I get more information on IPv6?	See www.ipv6.org for general information on IPv6. The KX III user guide describes the KX III's support for IPv6.

Servers

Question	Answer
Does Dominion KX III depend on a Windows server to operate?	Absolutely not. Because users depend on the KVM infrastructure to always be available in any scenario whatsoever (as they will likely need to use the KVM infrastructure to fix problems), Dominion KX III is designed to be completely independent from any external server.
What should I do to prepare a server for connection to Dominion KX III?	Set the mouse parameter options to provide users with the best mouse synchronization and turn off screensavers and any power management features that affect screen display.
What about mouse synchronization?	In the past, KVM-over-IP mouse synchronization was a frustrating experience. The Dominion KX III's Absolute Mouse Synchronization provides for a tightly synchronized mouse without requiring server mouse setting changes on Windows and Apple® Mac servers. For other servers, the Intelligent Mouse mode or the speedy, single mouse mode can be used to avoid changing the server mouse settings.
What comes in the Dominion KX III box?	The following is included: (1) Dominion KX III appliance, (2) Quick Setup Guide, (3) standard 19" rack mount brackets, (4) user manual CD-ROM, (6) localized AC line cord and (7) warranty certificate and other documentation.

Blade Servers

Question	Answer
Can I connect blade servers to the Dominion KX III?	Yes. Dominion KX III supports popular blade server models from the leading blade server manufacturers: HP®, IBM®, Dell® and Cisco®.
Which blade servers are supported?	The following models are supported: Dell PowerEdge® 1855, 1955 and M1000e; HP BladeSystem c3000 and c7000; IBM BladeCenter® H, E and S; and Cisco UCS B-Series.
Which CIM should I use?	It depends on the type of KVM ports on the specific make and model of the blade server you are using. The following CIMs are supported: DCIM-PS2, DCIM-USBG2, D2CIM-VUSB and D2CIM-DVUSB.
Which types of access and control are available?	The Dominion KX III provides automated and secure KVM access: (1) at the rack, (2) remotely over IP, (3) via CommandCenter and (4) by modem.
Do I have to use hotkeys to switch between blades?	Some blade servers require you to use hotkeys to switch between blades. With the Dominion KX III, you don't have to use these hotkeys. Just click on the name of the blade server, and the Dominion KX III will automatically switch to that blade without the explicit use of the hotkey.
Can I access the blade server's management module?	Yes. You can define the URL of the management module and access it from the Dominion KX III or from our CommandCenter Secure Gateway. If configured, one-click access is available.
How many blade servers can I connect to a Dominion KX III?	For performance and reliability reasons, you can connect up to eight blade chassis to a Dominion KX III, regardless of model. Raritan recommends connecting up to two times the number of remote connections supported by the device. For example, with a KX3-216 with two remote channels, we recommend connecting up to four blade server chassis. You can, of course, connect individual servers to the remaining server ports.

Question	Answer
I'm an enterprise customer using CommandCenter Secure Gateway. Can I access blade servers via CommandCenter Secure Gateway?	Yes. Once blade servers are configured on the Dominion KX III, the CommandCenter Secure Gateway user can access them via KVM connections. In addition, the blade servers are organized by chassis as well as CommandCenter Secure Gateway custom views.
What if I also want in-band or embedded KVM access?	In-band and embedded access to blade servers can be configured within CommandCenter Secure Gateway.
I'm running VMware® on some of my blade servers. Is this supported?	Yes. With CommandCenter Secure Gateway, you can display and access virtual machines running on blade servers.
Is virtual media supported?	This depends on the blade server. HP blades can support virtual media. The IBM BladeCenter (except for BladeCenter T) supports virtual media if configured appropriately. A virtual media CIM – D2CIM-VUSB or D2CIM-DVUSB – must be used.
Is Absolute Mouse Synchronization supported?	Servers with internal KVM switches inside the blade chassis typically do not support absolute mouse technology. For HP blade and some Dell blade servers, a CIM can be connected to each blade, so Absolute Mouse Synchronization is supported.
Is blade access secure?	Yes. Blade access uses all of the standard Dominion KX III security features such as 128-bit or 256-bit encryption. In addition, there are blade-specific security features such as per blade access permissions and hotkey-blocking that eliminates unauthorized access.
Does the Dominion KSX II or the KX III-101 support blade servers?	At this time, these products do not support blade servers.

Installation

Question	Answer
Besides the appliance itself, what do I need to order from Raritan to install Dominion KX III?	Each server that connects to Dominion KX III requires a Dominion or Paragon computer interface module (CIM), an adapter that connects directly to the keyboard, video and mouse ports of the server.
Which kind of Cat5 cabling should be used in my installation?	Dominion KX III can use any standard UTP (unshielded twisted pair) cabling, whether Cat5, Cat5e or Cat6. Often in our manuals and marketing literature, Raritan will simply say "Cat5" cabling for short. In actuality, any brand UTP cable will suffice for Dominion KX III.
Which types of servers and PCs can be connected to Dominion KX III?	Dominion KX III is completely vendor independent. Any server with standards-compliant keyboard, video and mouse ports can be connected. In addition, servers with serial ports can be controlled using the P2CIM-SER CIM.
How do I connect servers to Dominion KX III?	Servers that connect to the Dominion KX III require a Dominion or Paragon CIM, which connects directly to the keyboard, video and mouse ports of the server. Then, connect each CIM to Dominion KX III using standard UTP (unshielded twisted pair) cable such as Cat5, Cat5e or Cat6.
How far can my servers be from Dominion KX III?	In general, servers can be up to 150 feet (45 m) away from Dominion KX III, depending on the type of server. (See <i>Target Server Video Resolution Supported Connection Distances and Refresh Rates</i> (on page 421)) For the D2CIM-VUSB CIMs that supports virtual media and Absolute Mouse Synchronization, a 100-foot (30 m) range is recommended.

Question	Answer
Some operating systems lock up when I disconnect a keyboard or mouse during operation. What prevents servers connected to Dominion KX III from locking up when I switch away from them?	Each Dominion computer interface module (DCIM) dongle acts as a virtual keyboard and mouse to the server to which it is connected. This technology is called KME (keyboard/mouse emulation). Raritan's KME technology is data center grade, battle-tested and far more reliable than that found in lower-end KVM switches: it incorporates more than 15 years of experience and has been deployed to millions of servers worldwide.
Are there any agents that must be installed on servers connected to Dominion KX III?	Servers connected to Dominion KX III do not require any software agents to be installed because Dominion KX III connects directly via hardware to the servers' keyboard, video and mouse ports.
How many servers can be connected to each Dominion KX III appliance?	Dominion KX III models range from 8, 16 or 32 server ports in a 1U chassis, to 64 server ports in a 2U chassis. This is the industry's highest digital KVM switch port density.
What happens if I disconnect a server from Dominion KX III and reconnect it to another Dominion KX III appliance, or connect it to a different port on the same Dominion KX III appliance?	Dominion KX III will automatically update the server port names when servers are moved from port to port. Furthermore, this automatic update does not just affect the local access port, but propagates to all remote clients and the optional CommandCenter Secure Gateway management appliance.

Question	Answer
How do I connect a serially controlled (RS-232) device, such as a Cisco router/switch or a headless Sun server, to Dominion KX III?	If there are only a few serially controlled devices, they may be connected to a Dominion KX III using Raritan's P2CIM-SER serial converter. Customers can also consider deploying the Dominion KSX II, an integrated KVM and serial switch. The DKSX-144 features four KVM-over-IP ports and four serial ports. The DKSX-188 features eight KVM-over-IP ports and eight serial ports. However, if there are many serially controlled devices, we recommend the use of Raritan's Dominion SX line of secure console servers. Dominion SX offers more serial functionality at a better price point than Dominion KX III. This SX is easy to use, configure and manage, and can be completely integrated with a Dominion series deployment.

Local Port - KX III

Question	Answer
Can I access my servers directly from the rack?	Yes. At the rack, Dominion KX III functions just like a traditional KVM switch – allowing control of up to 64 servers using a single keyboard, monitor and mouse. You can switch between servers by the browser-based user interface or via a hotkey.
Can I consolidate the local ports of multiple KX IIIs?	Yes. You can connect the local ports of multiple KX III switches to another KX III using the "tiering" feature of the KX III. You can then access the servers connected to your KX III appliances from a single point in the data center via a consolidated port list.

Question	Answer
When I am using the local port, do I prevent other users from accessing servers remotely?	No. The Dominion KX III local port has a completely independent access path to the servers. This means a user can access servers locally at the rack – without compromising the number of users that access the rack remotely at the same time.
Can I use a USB keyboard or mouse at the local port?	Yes. The Dominion KX III has USB keyboard and mouse ports on the local port. Dominion KX III switches do not have PS/2 local ports. Customers with PS/2 keyboards and mice should utilize a PS/2 to USB adapter.
Is there an onscreen display (OSD) for local, at-the-rack access?	Yes, but Dominion KX III's at-the-rack access goes way beyond conventional OSDs. Featuring the industry's first browser-based interface for at-the-rack access, Dominion KX III's local port uses the same interface for local and remote access. Moreover, most administrative functions are available at the rack.
How do I select between servers while using the local port?	The local port displays the connected servers using the same user interface as the remote client. Users connect to a server with a simple click of the mouse or via a hotkey.
How do I ensure that only authorized users can access servers from the local port?	Users attempting to use the local port must pass the same level of authentication as those accessing remotely. This means that: If the Dominion KX III is configured to interact with an external RADIUS, LDAP or Active Directory® server, users attempting to access the local port will authenticate against the same server. If the external authentication servers are unavailable, Dominion KX III fails over to its own internal authentication database. Dominion KX III has its own stand-alone authentication, enabling instant, out-of-the-box installation.

Extended Local Port

Question	Answer
What is the extended local port?	The Dominion KX2-808, KX2-832 and KX2-864 featured an extended local port. The corresponding Dominion KX III models do not have an extended local port. Instead all KX III models have a tiering port. To extend the KX III's digital local port, you can use the Raritan Cat5 Reach DVI product for local and remote access up to 500 meters. See <i>Connecting a KX III and Cat5 Reach DVI - Provide Extended Local Port Functionality</i> (on page 398)

Dual Power Supplies

Question	Answer
Does Dominion KX III have a dual power option?	Yes. All Dominion KX III models come equipped with dual AC inputs and power supplies with automatic failover. Should one of the power inputs or power supplies fail, then the KX III will automatically switch to the other.
Does the power supply used by Dominion KX III automatically detect voltage settings?	Yes. Dominion KX III's power supply can be used in AC voltage ranges from 100–240 volts, at 50–60 Hz.
If a power supply or input fails, will I be notified?	The Dominion KX III front panel LED will notify the user of a power failure. An entry will also be sent to the audit log and displayed on the KX remote client user interface. If configured by the administrator, then SNMP or syslog events will be generated.

Intelligent Power Distribution Unit (PDU) Control

Question	Answer
What type of remote power control capabilities does Dominion KX III offer?	Raritan's intelligent PDUs can be connected to the Dominion KX III to provide power control of target servers and other equipment. For servers, after a simple one-time configuration step, just click on the server name to power on, off or to recycle a hung server.
What type of power strips does Dominion KX III support?	Raritan's Dominion PX™ and Remote Power Control (RPC) power strips. These come in many outlet, connector and amp variations. Note that you should not connect the PM series of power strips to the Dominion KX III as these power strips do not provide outlet-level switching.
How many PDUs can be connected to a Dominion KX III?	Up to eight PDUs can be connected to a Dominion KX III appliance.
How do I connect the PDU to the Dominion KX III?	The D2CIM-PWR is used to connect the power strip to the Dominion KX III. The D2CIM-PWR must be purchased separately; it does not come with the PDU.
Does Dominion KX III support servers with multiple power supplies?	Yes. Dominion KX III can be easily configured to support servers with multiple power supplies connected to multiple power strips. Four power supplies can be connected per target server.
Does the Dominion KX III display statistics and measurements from the PDU?	Yes. PDU-level power statistics, including power, current and voltage, are retrieved from the PDU and displayed to the user.
Does remote power control require any special configuration of attached servers?	Some servers ship with default BIOS settings such that the server does not automatically restart after losing and regaining power. For these servers, see the server's documentation to change this setting.
What happens when I recycle power to a server?	Note that this is the physical equivalent of unplugging the server from the AC power line, and reinserting the plug.

Ethernet and IP Networking

Question	Answer
What is the speed of Dominion KX III's Ethernet interfaces?	Dominion KX III supports gigabit as well as 10/100 Ethernet. KX III supports two 10/100/1000 speed Ethernet interfaces, with configurable speed and duplex settings (either auto detected or manually set).
Can I access Dominion KX III over a wireless connection?	Yes. Dominion KX III not only uses standard Ethernet, but also very conservative bandwidth with very high quality video. Thus, if a wireless client has network connectivity to a Dominion KX III, servers can be configured and managed at the BIOS level wirelessly.
Does the Dominion KX III offer dual gigabit Ethernet ports to provide redundant failover or load balancing?	Yes. Dominion KX III features dual gigabit Ethernet ports to provide redundant failover capabilities. Should the primary Ethernet port (or the switch/router to which it is connected) fail, Dominion KX III will failover to the secondary network port with the same IP address – ensuring that server operations are not disrupted. Note that automatic failover must be enabled by the administrator.
Can I use Dominion KX III with a VPN?	Yes. Dominion KX III uses standard Internet Protocol (IP) technologies from Layer 1 through Layer 4. Traffic can be easily tunneled through standard VPNs.
Can I use KX III with a proxy server?	Yes. KX III can be used with a SOCKS proxy server, assuming the remote client PC is configured appropriately. Contact the user documentation or online help for more information.
How many TCP ports must be open on my firewall in order to enable network access to Dominion KX III?	Two ports are required: TCP port 5000 to discover other Dominion appliances and for communication between Raritan appliances and CC-SG; and, of course, port 443 for HTTPS communication.
Are these ports configurable?	Yes. Dominion KX III's TCP ports are configurable by the administrator.

Question	Answer
Can Dominion KX III be used with Citrix®?	Dominion KX III may work with remote access products like Citrix if configured appropriately, but Raritan cannot guarantee it will work with acceptable performance. Customers should realize that products like Citrix utilize video redirection technologies similar in concept to digital KVM switches so that two KVM-over-IP technologies are being used simultaneously.
Can the Dominion KX III use DHCP?	DHCP addressing can be used; however, Raritan recommends fixed addressing since the Dominion KX III is an infrastructure appliance and can be accessed and administered more effectively with a fixed IP address.
I'm having problems connecting to the Dominion KX III over my IP network. What could be the problem?	The Dominion KX III relies on your LAN/WAN network. Some possible problems include: ▪ Ethernet auto-negotiation. On some networks, 10/100 auto-negotiation does not work properly, and the Dominion KX III appliance must be set to 100 Mb/full duplex or the appropriate choice for its network. ▪ Duplicate IP address. If the IP address of the Dominion KX III is the same as another appliance, network connectivity may be inconsistent. ▪ Port 5000 conflicts. If another appliance is using port 5000, the Dominion KX III default port must be changed (or the other appliance must be changed). ▪ When changing the IP address of a Dominion KX III, or swapping in a new Dominion KX III, sufficient time must be allowed for its IP and Mac® addresses to be known throughout the Layer 2 and Layer 3 networks.

Local Port Consolidation, Tiering and Cascading

Question	Answer
How do I physically connect multiple Dominion KX III appliances together into one solution?	To physically connect multiple KX III appliances together for consolidated local access, you can connect the Tiering ports of multiple "tiered" (or "cascaded") KX III switches to a "base" KX III using the Tiering port of the KX III. You can then access the servers connected to your KX III appliances from a single point in the data center via a consolidated port list. The Tiering port must be used to connect the tiered KX III switch to the base switch. Access via the consolidated port list is available in the data center or even from a remote PC. All servers connected to the tiered KX IIIs can be accessed via a hierarchical port list or via search (with wildcards). Two levels of tiering are supported; up to 1024 appliances can be accessed in a tiered configuration. Remote power control is also supported. Virtual media, smart card and blade server access via tiered access will be supported in a future release. Of course these features are available when accessed via a standard remote connection. While remote IP server access via the consolidated port list is available as a convenience, remote accessing a tiered server from CommandCenter or via the KX III the server is connected to, is recommended for optimal performance.

Question	Answer
Do I have to physically connect Dominion KX III appliances together?	Multiple Dominion KX III appliances do not need to be physically connected together. Instead, each Dominion KX III appliance connects to the network, and they automatically work together as a single solution if deployed with Raritan's CommandCenter Secure Gateway (CC-SG) management appliance. CC-SG acts as a single access point for remote access and management. CC-SG offers a significant set of convenient tools, such as consolidated configuration, consolidated firmware update and a single authentication and authorization database. Customers using CC-SG for centralized remote access can make good use of the KX III's tiering (cascading) feature to consolidate the local ports of multiple KX III switches and locally access up to 1024 servers from a single console when in the data center.
Is CC-SG required?	For customers wanting stand-alone usage (without a central management system), multiple Dominion KX III appliances still interoperate and scale together via the IP network. Multiple Dominion KX III switches can be accessed from the KX III Web-based user interface.

Question	Answer
Can I connect an existing analog KVM switch to Dominion KX III?	Yes. Analog KVM switches can be connected to one of Dominion KX III's server ports. Simply use a USB computer interface module (CIM), and attach it to the user ports of the existing analog KVM switch. Analog KVM switches supporting hotkey-based switching on their local ports can be tiered to a Dominion KX III switch and switched via a consolidated port list, both remotely and in the data center. Please note that analog KVM switches vary in their specifications and Raritan cannot guarantee the interoperability of any particular third-party analog KVM switch. Contact Raritan technical support for further information.

Computer Interface Modules (CIMs)

Question	Answer
What type of video is supported by your CIMs?	Our CIMs have traditionally supported analog VGA video. Three new CIMs support digital video formats, including DVI, HDMI and DisplayPort. These are the D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI and D2CIM-DVUSB-DP.

Question	Answer
Can I use computer interface modules (CIMs) from Paragon, Raritan's analog matrix KVM switch, with Dominion KX III?	Yes. Certain Paragon computer interface modules (CIMs) may work with Dominion KX IIXX IIII. (Please check the Raritan Dominion KX III Release Notes on the website for the latest list of certified CIMs.) However, because Paragon CIMs cost more than Dominion KX III CIMs (as they incorporate technology for video transmission of up to 1,000 feet [304 m]), it is not generally advisable to purchase Paragon CIMs for use with Dominion KX III. Also note that when connected to Dominion KX III, Paragon CIMs transmit video at a distance of up to 150 feet (46 m), the same as Dominion KX III CIMs – not at 1,000 feet (304 m), as they do when connected to Paragon.
Does Dominion KX III support Paragon Dual CIMs?	Yes. The Dominion KX III supports Paragon II Dual CIMs (P2CIM-APS2DUAL and P2CIM-AUSBDUAL), which can connect servers in the data center to two different Dominion KX III switches. If one KX III switch is not available, the server can be accessed through the second KX III switch, providing redundant access and doubling the level of remote KVM access. Please note these are Paragon CIMs, so they do not support the KX III advanced features such as virtual media, absolute mouse, audio, etc.

Security

Question	Answer
Is the Dominion KX III FIPS 140-2 Certified?	The Dominion KX III uses an embedded FIPS 140-2 validated cryptographic module running on a Linux platform per FIPS 140-2 implementation guidelines. This cryptographic module is used for encryption of KVM session traffic consisting of video, keyboard, mouse, virtual media and smart card data.
What kind of encryption does Dominion KX III use?	Dominion KX III uses industry-standard (and extremely secure) 256-bit AES, 128-bit AES or 128-bit encryption, both in its SSL communications as well as its own data stream. Literally no data is transmitted between remote clients and Dominion KX III that is not completely secured by encryption.
Does Dominion KX III support AES encryption as recommended by the U.S. government's NIST and FIPS standards?	Yes. The Dominion KX III utilizes the Advanced Encryption Standard (AES) for added security. 256-bit and 128-bit AES is available. AES is a U.S. government-approved cryptographic algorithm that is recommended by the National Institute of Standards and Technology (NIST) in the FIPS Standard 197.
Does Dominion KX III allow encryption of video data? Or does it only encrypt keyboard and mouse data?	Unlike competing solutions, which only encrypt keyboard and mouse data, Dominion KX III does not compromise security – it allows encryption of keyboard, mouse, video and virtual media data.
How does Dominion KX III integrate with external authentication servers such as Active Directory, RADIUS or LDAP?	Through a very simple configuration, Dominion KX III can be set to forward all authentication requests to an external server such as LDAP, Active Directory or RADIUS. For each authenticated user, Dominion KX III receives from the authentication server the user group to which that user belongs. Dominion KX III then determines the user's access permissions depending on the user group to which he or she belongs.

Question	Answer
How are usernames and passwords stored?	Should Dominion KX III's internal authentication capabilities be used, all sensitive information, such as usernames and passwords, is stored in an encrypted format. Literally no one, including Raritan technical support or product engineering departments, can retrieve those usernames and passwords.
Does Dominion KX III support strong passwords?	Yes. The Dominion KX III has administrator-configurable, strong password checking to ensure that user-created passwords meet corporate and/or government standards and are resistant to brute force hacking.
Can I upload my own digital certificate to the Dominion KX II/KX III?	Yes. Customers can upload self-signed or certificate authority-provided digital certificates to the Dominion KX III for enhanced authentication and secure communication.
Does the KX III support a configurable security banner?	Yes. For government, military and other security-conscious customers requiring a security message before user login, the KX III can display a user-configurable banner message and optionally require acceptance.
My security policy does not allow the use of standard TCP port numbers. Can I change them?	Yes. For customers wishing to avoid the standard TCP/IP port numbers to increase security, the Dominion KX III allows the administrator to configure alternate port numbers.

Smart Cards and CAC Authentication

Question	Answer
Does Dominion KX III support smart card and CAC authentication?	Yes. Smart cards and DoD common access cards (CAC) authentication to target servers is supported.

Question	Answer
What is CAC?	Mandated by Homeland Security Presidential Directive 12 (HSPD-12), CAC is a type of smart card created by the U.S. government and used by U.S. military and government staff. The CAC card is a multitechnology, multipurpose card; the goal is to have a single identification card. For more information, see the FIPS 201 standards.
Which KX III models support smart cards/CAC?	All Dominion KX III models are supported. The Dominion KX III-101 models do not currently support smart cards and CAC.
Do enterprise and SMB customers use smart cards, too?	Yes. However, the most aggressive deployment of smart cards is in the U.S. federal government.
Which CIMs support smart card/CAC?	The D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI and D2CIM-DVUSB-DP are the required CIMs.
Which smart card readers are supported?	The required reader standards are USB CCID and PC/SC. Consult the user documentation for a list of certified readers and more information.
Can smart card/CAC authentication work on the local port and via CommandCenter?	Yes. Smart card/CAC authentication works on both the local port and via CommandCenter. For the local port, connect a compatible smart card reader to the USB port of the Dominion KX III.

Manageability

Question	Answer
Can Dominion KX III be remotely managed and configured via Web browser?	Yes. Dominion KX III can be completely configured remotely via Web browser. Note that this does require that the workstation have an appropriate Java Runtime Environment (JRE) version installed. Besides the initial setting of Dominion KX III's IP address, everything about the solution can be completely set up over the network. (In fact, using a crossover Ethernet cable and Dominion KX III's default IP address, you can even configure the initial settings via Web browser.)
Can I back up and restore Dominion KX III's configuration?	Yes. Dominion KX III's appliance and user configurations can be completely backed up for later restoration in the event of a catastrophe. Dominion KX III's backup and restore functionality can be used remotely over the network, or through your Web browser.
What auditing or logging does Dominion KX III offer?	For complete accountability, Dominion KX III logs all major user events with a date and time stamp. For instance, reported events include (but are not limited to): user login, user logout, user access of a particular server, unsuccessful login, configuration changes, etc.
Can Dominion KX III integrate with syslog?	Yes. In addition to Dominion KX III's own internal logging capabilities, Dominion KX III can send all logged events to a centralized syslog server.
Can Dominion KX III integrate with SNMP?	Yes. In addition to Dominion KX III's own internal logging capabilities, Dominion KX III can send SNMP traps to SNMP management systems. SNMP v2 and v3 are supported.
Can an administrator log-off a user?	Yes, administrators can view which users are logged into which ports and can log-off a user from a specific port or from the appliance if required.

Question	Answer
Can Dominion KX III's internal clock be synchronized with a timeserver?	Yes. Dominion KX III supports the industry-standard NTP protocol for synchronization with either a corporate timeserver, or with any public timeserver (assuming that outbound NTP requests are allowed through the corporate firewall).

Documentation and Support

Question	Answer
Is online help available?	Yes. Online help is available from the KX III user interface, and at raritan.com with the documentation. Online help includes KX III administration and end user information on using the Remote Console, Virtual KVM Client (VKC) Active KVM Client (AKC) and Local Console, as well KX III specifications, informational notes, using KX III with Paragon II, connecting KX III to the Cat5 Reach DVI, connecting KX III to the T1700-LED, and so on.
Where do I find documentation on the Dominion KX III?	The documentation is available at raritan.com. The documentation is listed by firmware release.
What documentation is available?	A Quick Setup Guide, online help, a PDF version of the help in the form of an Administrators Guide and a Users Guide, as well as Release Notes and other information are available.
What CIM should I use for a particular server?	Consult the CIM Guide available with the KX III documentation. Note that DVI, HDMI and DisplayPort video standards are supported with the digital video CIMs.
How long is the hardware warranty for the KX III?	The Dominion KX III comes with a standard two-year warranty, which can be extended to 5 years of warranty coverage.

Miscellaneous

Question	Answer
What is Dominion KX III's default IP address?	192.168.0.192
What is Dominion KX III's default username and password?	The Dominion KX III's default username and password are admin/raritan. However, for the highest level of security, the Dominion KX III forces the administrator to change the Dominion KX III default administrative username and password when the appliance is first booted up. Username is not case sensitive.
I changed and subsequently forgot Dominion KX III's administrative password; can you retrieve it for me?	Dominion KX III contains a hardware reset button that can be used to factory reset the appliance, which will reset the administrative password on the appliance to the default password.
How do I migrate from the Dominion KX II to Dominion KX III?	In general, KX II customers can continue to use their existing switches for many years. As their data centers expand, customers can purchase and use the new KX III models. Raritan's centralized management appliance, CommandCenter Secure Gateway (CC-SG) Release 6.0 supports KX II and KX III switches seamlessly.
Will my existing KX II CIMs work with Dominion KX III switches?	Yes. Existing KX II CIMs will work with the Dominion KX III switch. In addition, select Paragon CIMs will work with the KX III. This provides an easy migration to KX III for Paragon II customers who wish to switch to KVM over IP. However, you may want to consider the D2CIM-VUSB and D2CIM-DVUSB CIMs that support virtual media, audio and Absolute Mouse Synchronization. Additionally, digital video CIMs supporting DVI, HDMI, and Display Port are also available.

Index

A

A

- AC Power • 36
- About the Cat5 Reach DVI • 398
- Absolute Mouse Mode • 370, 371
- Absolute Mouse Synchronization • 275, 319
- Accent Symbol (Windows XP Operating System Clients Only) • 456
- Access a Target Server from the KX III • 48
- Access a Virtual Media Drive on a Client Computer • 247
- Access and Control Target Servers Remotely • 48
- Access and Copy Connection Information • 261, 264
- Access and Display Favorites • 382
- Access Connection Properties • 260
- Access the Port Configuration Page • 96
- Accessing a Blade Chassis from a Base Device • 148
- Accessing a Paragon II from the KX III • 402
- Accessing a Target Server • 385
- Accessing the KX III Using CLI • 226
- Accessing Virtual Media on a Windows 2000 • 451
- Active KVM Client (AKC) Help • 8, 119, 301, 468
- Active System Partition • 252
- Active System Partitions • 250
- Add New Macro • 314
- Adding a New User • 70, 73
- Adding a New User Group • 63, 70
- Adding Attributes to the Class • 411
- Adding Scripts • 179
- Additional Security Warnings • 11, 12
- Additional Supported Mouse Settings • 30, 33
- Adjust Audio Settings • 299
- Adjusting Capture and Playback Buffer Size (Audio Settings) • 299
- Adjusting Video Settings • 271
- Administering the KX III Console Server Configuration Commands • 231

- AKC Download Server Certification Validation IPv6 Support Notes • 446
- AKC Supported Browsers • 302
- AKC Supported Microsoft .NET Framework • 301
- AKC Supported Operating Systems • 302
- Allow Cookies • 302
- Allow Pop-Ups • 10
- Apple Mac Mouse Settings • 35
- Apply a Native Display Resolution to Other CIMs • 103, 105
- Apply Selected Profiles to Other CIMs • 103, 104
- Applying and Removing Scripts • 178, 182
- Applying KX III Appliance Setting to a KX III Using a Backup/Restore File • 207, 210
- Assign the KX III a Device Name • 39
- Associating Outlets with Target Devices • 109
- Audio • 292, 460
- Audio in a Linux Environment • 460
- Audio in a Mac Environment • 433
- Audio in a Windows Environment • 461
- Audio Level • 293, 432
- Audio Menu • iii, 332
- Audio Playback and Capture Issues • 460
- Audio Playback and Capture Recommendations and Requirements • 293, 297, 432
- Audio Settings • 333
- Audit Log • 205, 396, 397
- Authentication Settings • 74
- Authentication When Accessing a Smart Card Reader • 289
- Auto Sense • 324
- Auto-Sense Video Settings • 270, 372
- Available USB Profiles • 55

B

- B. Network Ports • 37
- Bandwidth and KVM-over-IP Performance • 470
- Bandwidth Requirements • 294, 432
- Before Creating a Tiering Configuration • 145

Black Stripe/Bar(s) Displayed on the Local Port • 455

Blade Chassis - Port Access Page • 22

Blade Chassis Configuration Options • 115

Blade Chassis Sample URL Formats • 121, 125, 127, 136

Blade Servers • 476

Browser Notes • 461

BSMI Certification • 443

Build a New Macro • 267

C

C

Local User Port (Local Console) • 37

Calibrating Color • 271

Cannot Connect to Drives from Linux Clients • 449

Cannot Write To/From a File from a Mac Client • 449

Caret Symbol (Linux Clients Only) • 456

CC-SG Notes • 461

Certified Modems • 156, 434

Change the Default Password • 39

Change the Keyboard Layout Code (Sun Targets) • 50

Changing a Password • 86, 380

Changing a USB Profile when Using a Smart Card Reader • 454

Changing the Default GUI Language Setting • 186

Checking Your Browser for AES Encryption • 194, 195

Choose Failover or Isolation Mode • 37, 39, 87

CIM Compatibility • 54

CIM Notes • 447

CIMs Required for Dual Video Support • 235, 292

CIMs Required for Virtual Media • 244

Cisco ACS 5.x for RADIUS Authentication • 82

Clear Video Settings Cache • 271, 325, 328

CLI Commands • 226, 230

CLI Prompts • 230

CLI Syntax -Tips and Shortcuts • 228

Client Launch Settings • iii, 281

Collect a Diagnostic Snapshot from VKC, VKCS, and AKC • 285

Collecting a Diagnostic Snapshot of the Target • 284

Color Accuracy • 261, 308

Color Calibration • 325

Command Line Interface (CLI) • 226

Command Line Interface High-Level Commands • 348

Command Line Interface Shortcuts • 348

Common Commands for All Command Line Interface Levels • 228

Completion of Commands • 227

Computer Interface Modules (CIMs) • 489

Conditions when Read/Write is Not Available • 246, 248

Configure and Test SMTP Server Settings • 172, 173

Configure Date/Time Settings • 46

Configure DSAM Serial Ports • 338

Configure KX III for Dual LAN Failover Mode • 39, 40, 87, 94

Configure KX III for Dual LAN Isolation Mode • 39, 41, 87, 89

Configure Local Console Scan Settings • 283, 390, 392

Configure Port Scan • 283

Configure Serial Port Keyword List • 342

Configure Settings to Access KX III via Modem through Direct Port Access • 159

Configure the CIM Power Associations • 103

Configure the CIM Settings • 103

Configure the CIM Target Settings • 103, 419

Configure the DNS Settings • 91

Configure the Local Port Scan Mode Settings • 140

Configure the Power Save Feature (Optional) • 142, 224

Configuring and Enabling Tiering • 38, 67, 70, 139, 145

Configuring Blade Chassis • 110

Configuring CIM Ports • 102, 425, 426, 454

Configuring Connection Properties • 156, 260, 264

Configuring Date/Time Settings • 165, 201

Configuring Event Management - Destinations • 155, 166, 168, 175

- Configuring Event Management - Settings • 166
 - Configuring IP Access Control • 198
 - Configuring KVM Switches • 100, 145
 - Configuring KX III Local Port Settings • 139, 145
 - Configuring KX III Local Port Settings from the Local Console • 222
 - Configuring Modem Settings • 38, 156
 - Configuring Network • 231
 - Configuring Port Scan Settings in VKC/VKCS and AKC • 283, 376, 378, 390, 392
 - Configuring Ports • 96
 - Configuring Rack PDU (Power Strip) Targets • 105
 - Configuring SNMP Agents • 154, 167
 - Configuring SNMP Traps • 155, 166, 167
 - Configuring Standard Target Servers • 99, 145, 240
 - Configuring USB Profiles (Port Page) • 61, 126, 137
 - Connect • 24
 - Connect and Disconnect Scripts • 178
 - Connect and Enable Global Access to an External USB-Connected Broadband Modem • 157
 - Connect Audio • 332
 - Connect Cat5 Reach DVI and Cat5 Reach DVI • 399
 - Connect Drive Permissions (Linux) • 251
 - Connect Drive Permissions (Mac) • 253
 - Connect Files and Folders • 329
 - Connect ISO • 330
 - Connect Key Examples • 142, 224, 387
 - Connect KX III and DSAM • 336
 - Connect to a Digital Audio Device • 297
 - Connect to a DVI Monitor • 37
 - Connect to a Target from Virtual KVM Client (VKC), Standalone VKC (VKCs), or Active KVM Client (AKC) • 259, 304
 - Connect to a Target Using the Mobile KVM Client • 364, 365
 - Connect to a VGA Monitor (Optional) • 30, 38
 - Connect to DSAM Serial Target via SSH • 350
 - Connect to DSAM Serial Target with URL Direct Port Access • 349
 - Connect to DSAM Serial Targets with KX3 GUI • 348
 - Connect to Virtual Media • 288
 - Connecting a KX III and Cat5 Reach DVI - Provide Extended Local Port Functionality • 398, 483
 - Connecting a Rack PDU • 105
 - Connecting and Disconnecting from a Digital Audio Device • 296, 297
 - Connecting and Disconnecting from Virtual Media • 247
 - Connecting the Paragon II to the KX III • 408
 - Connecting to Multiple Targets from a Single Remote Client • 296, 297
 - Connection Info • 311
 - Connection Information • 264
 - Connection Properties • 307
 - Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional) • 16
 - Copy and Paste • 356
 - Create a Backup File • 208, 210
 - Create User Groups and Users • 47
 - Creating a Dual Video Port Group • 150, 151, 183, 185, 240, 242
 - Creating a KX III Backup and Restore File • 207
 - Creating a New Attribute • 410
 - Creating Port Groups • 183, 184
- ## D
- D. Local DVI-D Port • 37
 - Default Connection Properties • 307, 311
 - Default Connection Property Settings - Optimized for Best Performance • 260
 - Delete a Macro • 315
 - Dell • 115
 - Dell Blade Chassis Configuration • 119
 - Dell Chassis Cable Lengths and Video Resolutions • 110, 119, 123, 428
 - Device Diagnostics • 220
 - Device Information • 206
 - Device Management • 87
 - Device Services • 120, 124, 143
 - Diagnostics • 217
 - Digital Audio • 291

Digital Audio VKC and AKC Icons • 293
 Digital CIM Established and Standard Modes • 424, 425
 Digital CIM Established Modes • 426
 Digital CIM Standard Modes • 426
 Digital CIM Timing Modes • 425
 Direct Port Access and Dual Port Video Groups • 242
 Direct Port Access URL Syntax for the Active KVM Client (AKC) • 150
 Direct Port Access URL Syntax for the Virtual KVM Client (VKC) • 149
 Disable Java Caching and Clear the Java Cache • 444
 Disable 'Protected Mode' • 303
 Disconnect • 25
 Disconnect from a Target Server • 49
 Disconnect from an Audio Device • 298
 Disconnect from Virtual Media Drives • 249
 Disconnecting Mac and Linux Virtual Media USB Drives • 451
 Disconnecting Users from Ports • 71, 72, 73
 Discovering Devices on the KX III Subnet • 383
 Discovering Devices on the Local Subnet • 382
 Display Connection Info • 368, 372
 Display Mobile Device Keyboard • 367, 368
 DKX3-808 Fast Switching • 27, 49
 Documentation and Support • 495
 Dominion KX III User Station • 8, 19, 48, 360
 Dominion KX3-832 • 5
 Dominion KX3-864 • 6
 Drive Partitions • 250, 252
 DSAM LED Operation • 336
 Dual Mouse Modes • 275
 Dual Port Video Configuration Steps • 233, 238
 Dual Port Video Group Usability Notes • 235
 Dual Port Video Groups - Port Access Page • 22
 Dual Port Video Groups Displayed on the Ports Page • 242
 Dual Power Supplies • 483
 Dual Stack Login Performance Issues • 447
 Dual Video Port Group Supported Mouse Modes • 234, 240, 292
 Dual Video Port Groups • 233
 DVI Compatibility Mode • 426

E

E. Connect Target Servers to KX III • 38
 Editing rcusergroup Attributes for User Members • 413
 Emulator • 352
 Enable AKC Download Server Certificate Validation • 303
 Enable Direct Port Access • 151
 Enable Email (SMTP) Notifications from the Remote Console • 172
 Enable Favorites • 381
 Enable Local Port Device Tiering • 139, 145
 Enable Standalone VKC Download Server Certificate Validation • 153
 Enable Standard Local Port • 139
 Enabling Direct Port Access via URL • 149, 242, 301
 Enabling FIPS 140-2 • 194, 196
 Enabling SSH • 143
 Enabling the AKC Download Server Certificate Validation • 152
 Enabling Tiering • 145, 147
 Enabling TLS Protocols • iii, 197
 Encryption and Share • iii, 193, 197, 397
 Enter Intelligent Mouse Mode • 275
 Entering the Discovery Port • 144
 Ethernet and IP Networking • 485
 Event Management • 166
 Events Captured in the Audit Log and Syslog • 205, 442
 Example 1
 Import the Certificate into the Browser • 12, 15
 Example 2
 Add the KX III to Trusted Sites and Import the Certificate • 14
 Example Dual Port Video Group Configuration • 237
 Export Macros • 269
 Extended Local Port • 482

F

F. Tiering (Optional) • 38
 Factory Default Login Information • 10, 32

- FIPS 140-2 Support Requirements • 197
- Firmware Upgrade • 213
- Forward Mount • 31
- French Keyboard • 456
- Frequently Asked Questions • 462
- From LDAP/LDAPS • 409
- From Microsoft Active Directory • 409
- Full Screen Mode • 288

G

- G. Connect the Modem (Optional) • 38
- General FAQs • 462
- General Settings • 278
- Generic • 115
- Generic Blade Chassis Configuration • 110
- Get Started Using KX III • 10, 229
- Group-Based IP ACL (Access Control List) • 63, 67, 69, 198

H

- Handling Conflicts in Profile Names • 212
- Hardware • 2, 416
- Help Choosing USB Profiles • 452
- Hot Key Sequences to Access Blade Chassis • 117
- HP • 115
- HP and Cisco UCS Blade Chassis Configuration (Port Group Management) • 129, 131, 183, 184
- HSC Functions • 352
- HTML KVM Client (HKC) Help • iii, 8, 241, 255, 305
- HTML Serial Console (HSC) Help • 349, 351
- HTTP and HTTPS Port Settings • 144

I

- IBM • 115
- IBM AIX Mouse Settings • 36
- IBM Blade Chassis Configuration • 123
- Implementing LDAP/LDAPS Remote Authentication • 75
- Implementing RADIUS Remote Authentication • iii, 80
- Import and Export Macros • iii, 314, 316
- Import Macros • 268

- Importing and Exporting Macros • 268
- Importing and Exporting Scripts • 179, 182
- Include KX III IP Address in 'Trusted Sites Zone' • 302
- Informational Notes • 434, 444
- Initial Configuration Using CLI • 229
- Input Menu • 312
- Install and Configure KX III • 10
- Installation • 478
- Installing a Certificate • 11, 12
- Intelligent • 319
- Intelligent Mouse Mode • 275, 370, 371
- Intelligent Mouse Synchronization Conditions • 276, 319, 322
- Intelligent Power Distribution Unit (PDU) Control • 483
- Interface Command • 232
- Introduction • 1
- IPv6 Command • 233
- IPv6 Networking • 474
- IPv6 Support Notes • 446

J

- Java Not Loading Properly on Mac • 445
- Java Runtime Environment (JRE) Notes • 441, 444
- Java Validation and Access Warning • 11
- JRE Requirements and Browser Considerations for Mac • 439

K

- Keyboard • 266
- Keyboard Language Preference (Fedora Linux Clients) • 457
- Keyboard Languages • 369
- Keyboard Layout • iii, 312
- Keyboard Limitations • 280
- Keyboard Macros • 267
- Keyboard Notes • 456
- KX III Device Photos and Features • 2
- KX III Dimensions and Physical Specifications • 416
- KX III Installation and Configuration • 30
- KX III Interface and Navigation • 19
- KX III KVM Client Applications • 8

KX III KVM Client Launching • 18, 48, 255, 305
 KX III KVM Clients • 18, 48, 255
 KX III Local Console • 30, 221, 385
 KX III Local Console - Administration
 Functions • 8, 221
 KX III Local Console Factory Reset • 396
 KX III Local Console Interface • 8, 30
 KX III Online Help • 9
 KX III Remote Console • 374
 KX III Remote Console Interface • 8, 20, 374
 KX III Remote/Local Console Interfaces and
 User Station • 8
 KX III Supported Keyboard Languages • 434
 KX III Supported Local Port DVI Resolutions •
 104, 114, 386, 420
 KX III Supported Target Server Video
 Resolutions • 33, 238, 419, 421
 KX III Virtual Media Prerequisites • 244
 KX III-to-KX III Paragon CIM Guidelines • 405
 KX III-to-Paragon II Guidelines • 406
 KX II-to-KX III Unsupported Backup/Restore
 File Settings and Functions • 209, 210, 211
 KX3-832 Features • 5
 KX3-832 Photos • 5
 KX3-864 Features • 6
 KX3-864 Photos • 6

L

Launch Keyboard Macro • 370
 LED Statuses During KX III Boot Up • 30, 36
 Left Panel • 28, 168
 Link to a Blade Chassis Interface - Blade
 Chassis Managed Links • 118
 Linux Mouse Settings • 35
 List of KX III SNMP Traps • 155, 167, 169
 Local Console Smart Card Access • 289, 394
 Local Console USB Profile Options • 395
 Local Console Video Resolution Behavior • 386
 Local Port - KX III • 481
 Local Port Auto-Sense (Video Refresh) -
 Default Hot Key • 387
 Local Port Consolidation, Tiering and
 Cascading • 486
 Local Port Hot Keys and Connect Keys • 386
 Local Port Requirements • 429
 Logging In • 226, 227

Logging In to KX III • 18, 362, 374
 Logging Users Off the KX III (Force Logoff) • 71,
 72, 73
 Login Limitations • 187, 188

M

Mac Keyboard Keys Not Supported for Remote
 Access • 459
 Mac Mini BIOS Keystroke Commands • 435
 Macro Editor • 314
 Macros Not Saving on Linux Targets • 458
 Maintenance • 205
 Make a Power Association • 109
 Manage Mobile Client Keyboard Macros • 364,
 369, 370
 Manageability • 493
 Managing Blade Chassis • 119
 Managing Favorites • 29, 301, 381
 Manual and Auto-Discovery Blade Chassis
 Configuration • 116
 Mapped Drives • 250
 Miscellaneous • 496
MKC Toolbar Icons • 366
 Mobile KVM Client (MKC) Help • 8, 19, 364
 Modifying an Existing User • 73
 Modifying an Existing User Group • 69
 Modifying Scripts • 182
 Mount a Smart Card Reader • 290
 Mounting CD-ROM/DVD-ROM/ISO Images •
 248, 253
 Mounting Local Drives • 245
 Mouse Modes • 318
 Mouse Modes when Using the Mac Boot Menu
 • 58, 60, 137
 Mouse Notes • 459
 Mouse Options • 274
 Mouse Pointer Synchronization (Fedora) • 459
 Mouse Settings • 33
 Mouse Sync • 321
 Mouse Sync Issues in Mac OS 10 • 459
 Mouse Synchronization Tips • 277
 Moving Between Ports on a Device • 461
 Multi-Language Keyboard JRE Requirement •
 441

N

Name Command • 233
 Name Your Target Servers • 44
 Naming the Rack PDU (Port Page for Power Strips) • 107
 Navigating the CLI • 227
 Network Interface Page • 217
 Network Settings • 87
 Network Speed Settings • 94, 427
 Network Statistics Page • 217
 Noise Filter • 263, 310
 Note on Microsoft Active Directory • 48
 Note to CC-SG Users • 47
 Notes on Mounting Local Drives • 245
 Number of Supported Audio/Virtual Media and Smartcard Connections • 434
 Number of Supported Virtual Media Drives • 247
 Numeric Keypad • 456

O

Operating System Audio Playback Support • 297
 Operating System IPv6 Support Notes • 446
 Operating the User Station • 362
 Optimize for
 Selections • 261
 Overview • 1, 19, 30, 51, 54, 226, 243, 256, 301, 361, 374, 385, 402, 444

P

Package Contents • 2
 PC Share Mode and Privacy Settings when Using Smart Cards • 289
 Permissions and Dual Video Port Group Access • 186, 236
 Permitted KX III Tiering Configurations • 145
 Ping Host Page • 218
 Port Access Page (Remote Console Display) • 21, 110, 374
 Port Action Menu • 21, 24, 259, 304
 Port Configuration Page • 97
 Port Group Management • 183
 Port Name • 98

Port Number • 97
 Port Type • 99
 Power Control from Tiered Devices • 149
 Power Control Menu • iii, 334
 Power Control Using VKC, VKCS, and AKC • 26, 27, 52, 300
 Power Cycle • 27
 Power Cycle a Target • 359
 Power Off • 26
 Power Off a Target • 359
 Power On • 26
 Power on a Target • 358
 Power Status • 358
 Power Supply Setup • 176
 Powerstrip is not detected • 449
 Prerequisites for Using AKC • 301, 302
 Prerequisites for Using Virtual Media • 244
 Proxy Server Configuration for Use with VKC, VKCS, and AKC • 258, 303

R

Rack Mounting • 31
 Rack PDU (Power Strip) Outlet Control • 51
 RADIUS Communication Exchange
 Specifications • 83
 RADIUS Using RSA SecurID Hardware Tokens • 84
 Raritan Client Navigation when Using Dual Video Port Groups • 241
 Rear Mount • 31
 Rebooting the KX III • 214
 Recommendations for Audio Connections when PC Share Mode is Enabled • 294, 432
 Recommendations for Dual Port Video • 234, 292
 Recommended Minimum Active KVM Client (AKC) Requirements • 301
 Recommended Minimum Virtual KVM Client (VKC) Requirements • 256
 Refresh Screen • 323
 Refreshing the Screen • 270
 Relationship Between Users and Groups • 63
 Remote Access • 465
 Remote and Local Access from Tiered Devices • 148
 Remote Client Requirements • 430

Remote Linux Client Requirements • 430
 Remote PC VM Prerequisites • 244
 Remotely Access Targets Using a Mobile Device • 364
 Remove a Power Association • 109
 Required and Recommended Blade Chassis Configurations • 110, 119, 123, 134
 Requirements to Apply a KX II Backup and Restore File to a KX III • 209, 210
 Reset Network Settings to Factory Defaults • 95
 Resetting the KX III Using the Reset Button on the Device • 195, 397
 Resolving Issues with Firefox Freezing when Using Fedora • 461
 Restore Your KX III Using a Restore File • 209, 210
 Return to the Local Console from a Target Device - Default Hot Key • 387
 Returning User Group Information • 409
 Returning User Group Information from Active Directory Server • 79
 Returning User Group Information via RADIUS • 83
 Root User Permission Requirement • 250

S

Saving Audio Settings • 296, 297
 Scaling • 287
 Scan for Targets • 379
 Scan for Targets - Local Console • 393
 Scanning Port Slide Show - Local Console • 390
 Scanning Ports - Local Console • 376, 389
 Scanning Ports - Remote Console • 21, 24, 242, 283, 375, 389
 Scanning Ports Slide Show - Remote Console • 376
 Screenshot • 323
 Screenshot from Target Command (Target Screenshot) • 273
 Security • 490
 Security and Authentication • 221
 Security Banner • 203
 Security Issues • 231
 Security Management • 187

Security Settings • 70, 187
 Security Warnings and Validation Messages • 11, 12, 18
 Select the Local Console Keyboard Type • 140, 222
 Select the Local Port Connect Key • 142, 224, 386
 Select the Local Port Hotkey • 141, 223, 386
 Select the Local User Authentication • 143, 225
 Selecting Profiles for a KVM Port • 61
 Send Ctrl+Alt+Del Macro • 266
 Send LeftAlt+Tab (Switch Between Open Windows on a Target Server) • 266
 Send Macro • iii, 313
 Send Smart Card Remove and Reinsert Notifications • 291
 Send Text File • 356
 Send Text to Target • iii, 266, 317
 Serial Access With Dominion Serial Access Module • 335
 Servers • 476
 Set Keyboard Type • 369
 Set Mouse Mode • 370
 Set Scan Tab • 24
 Set Video Connection Quality • 368, 372
 Setting CIM Keyboard/Mouse Options • 266
 Setting Network Parameters • 229
 Setting Parameters • 229
 Setting Permissions • 63, 64, 69
 Setting Permissions for an Individual Group • 67, 70
 Setting Port Permissions • 63, 66, 69
 Setting the Registry to Permit Write Operations to the Schema • 410
 Simultaneous Users • 386
 Single • 320
 Single Mouse Mode • 278
 Single Mouse Mode when Connecting to a Target Under CC-SG Control • 459
 Smart Card Minimum System Requirements • 289, 394, 429
 Smart Card Minimum System Requirements, CIMs and Supported/Unsupported Smart Card Readers • 289
 Smart Card Notes • 461

- Smart Card Reader Detected • 290
 - Smart Cards • 289
 - Smart Cards and CAC Authentication • 492
 - Software • 3, 438
 - Special Sun Key Combinations • 388
 - Specifications • 416
 - Specify Power Supply Autodetection • 44
 - SSH Access from a UNIX/Linux Workstation • 227
 - SSH Access from a Windows PC • 226
 - SSH Connection to the KX III • 226
 - SSL and TLS Certificates • iii, 11, 51, 200, 307
 - Standard • 320
 - Standard Mouse Mode • 277, 370, 371
 - Step 1
 - Configure the Target Server Display • 238
 - Configuring Network Firewall Settings • 32
 - Step 2
 - Configuring KVM Target Servers • 33
 - Connect the Target Server to the KX III • 239
 - Step 3
 - Configure the Mouse Mode and Ports • 240
 - Connecting the Equipment • 36, 99
 - Step 4
 - Configuring the KX III • 38
 - Create the Dual Video Port Group • 239, 240
 - Step 5
 - Launch a Dual Port Video Group • 241
 - Launching the KX III Remote Console • 48
 - Step 6
 - Configuring the Keyboard Language (Optional) • 30, 50
 - Step 7
 - Create and Install an SSL Certificate • 51
 - Stopping CC-SG Management • 216
 - Strong Passwords • 86, 187, 190, 380
 - Sun Composite Synch Video • 455
 - Sun Solaris Mouse Settings • 35
 - Supported Audio Device Formats • 292
 - Supported Blade Chassis Models • 110, 119, 123, 131
 - Supported CIMs for Blade Chassis • 110, 119, 123, 131
 - Supported CLI Commands • 344
 - Supported Computer Interface Module (CIMs) Specifications • 35, 54, 235, 289, 421
 - Supported Connection Distances Between Paragon II and KX III • 408
 - Supported Digital Video CIMs for Mac • 424
 - Supported Number of Ports and Remote Users per Model • 7
 - Supported Operating Systems, Browsers and Java Versions • 438
 - Supported Paragon II CIMS and Configurations • 403
 - Supported Protocols • 47
 - Supported Remote Connections • 427
 - Supported Smart Card Readers • 394, 430
 - Supported Tasks Via Virtual Media • 245
 - Supported USB Device Combinations • 337
 - Supported Virtual Media Operating Systems • 246
 - Supported Virtual Media Types • 246
 - SUSE/VESA Video Modes • 455
 - Switch between Target Servers • 49
 - Switch From • 25
 - Sync Mouse in Intelligent or Standard Mouse Mode • 372**
 - Synchronize Your Mouse • 277
 - SysLog Configuration • 174
- ## T
- Target BIOS Boot Time with Virtual Media • 451
 - Target Server Requirements • 429
 - Target Server Video Resolution Supported Connection Distances and Refresh Rates • 421, 479
 - Target Server Video Resolutions • 33
 - Target Server VM Prerequisites • 244
 - Target Status Indicators During Port Scanning
 - Local Console • 392
 - Target Status Indicators During Port Scanning
 - Remote Console • 377
 - Target Video Picture Not Centered (Mouse Out of Synch) • 449
 - TCP and UDP Ports Used • 437
 - TCP Port 443 • 33
 - TCP Port 5000 • 32
 - TCP Port 80 • 33

Text Readability • 261, 308
 Tiered Devices - Port Access Page • 21
 Tiered KX III Connection Example • 146
 Tilde Symbol • 457
 Tips for Adding a Web Browser Interface • 114,
 121, 123, 125, 127, 128, 447
 Tool Options • 278, 288
 Touch Mouse Functions • 364, 365, 373
 Trace Route to Host Page • 219
 Turning Outlets On/Off and Cycling Power • 52

U

Universal Virtual Media • 468
 Unmount (Remove) a Smart Card Reader •
 291
 Unsupported and Limited Features on Tiered
 Targets • 146
 Unsupported Smart Card Readers • 394, 431
 Update a Smart Card Reader • 291
 Updating the LDAP Schema • 409
 Updating the Schema Cache • 413
 Upgrade DSAM Firmware • 342
 Upgrade History • 214
 Upgrading CIMs • 137, 212
 Upgrading the KX III Firmware • 213
 USB Port and Profile Notes • 452
 USB Profile • 312
 USB Profile Management • 211, 212
 USB Profiles • 54, 137, 265
 User Authentication Process • 85
 User Blocking • 187, 191
 User Group List • 62
 User Groups • 61
 User Management • 61, 221
 User Station Photo and Features • 362
 Users • 70
 Using a Windows Keyboard to Access Mac
 Targets • 437
 Using Scan Port Options • 378
 Using the MKC Toolbar • 366, 367

V

Version Information - Virtual KVM Client • 300
 Video Image Appears Dark when Using a Mac
 • 454

Video Menu • 323
 Video Mode • 262, 309
 Video Mode and Resolution Notes • 386, 454
 Video Properties • 270
 Video Settings • 325
 Video Shrinks after Adjusting Target Clock •
 454
 View and Edit LAN Interface Settings • 93
 View by Group Tab • 23
 View by Search Tab • 23
 View by Serial Tab • 23
 View DSAM Serial Ports • 338
 View Menu • 328
 View MKC Help • 373
 View Options • 287
 View Status Bar • 287
 View the KX III Users List • 71
 View Toolbar • 287
 View Users by Port • 71
 Viewing the KX III MIB • 154, 167, 174
 Virtual KVM Client (VKC and VKCs) Help • 8,
 119, 256, 301, 468
 Virtual KVM Client (VKC) Smart Card
 Connections to Fedora Servers • 461
 Virtual KVM Client (VKC), VKCS, and Active
 KVM Client (AKC) Requirements • 440
 Virtual KVM Client Java Requirements • 257
 Virtual KVM Client Version Not Known from
 CC-SG Proxy Mode • 461
 Virtual Media • 243, 288
 Virtual Media Connection Failures Using High
 Speed for Virtual Media Connections • 452
 Virtual Media File Server Setup (File Server
 ISO Images Only) • 253, 331
 Virtual Media in a Linux Environment • 250
 Virtual Media in a Mac Environment • 252
 Virtual Media in a Windows XP Environment •
 249
 Virtual Media Linux Drive Listed Twice • 451
 Virtual Media Menu • iii, 329
 Virtual Media Not Refreshed After Files Added
 • 451
 Virtual Media Notes • 449
 Virtual Media via VKC and AKC in a Windows
 Environment • 450
 VM-CIMs and DL360 USB Ports • 452

W

- Welcome • iii
- Windows 2000 Composite USB Device
 - Behavior for Virtual Media • 448
- Windows 2000 Mouse Settings • 34
- Windows 3-Button Mouse on Linux Targets •
447
- Windows 7 and Windows Vista Mouse Settings
 - 34
- Windows XP, Windows 2003, Windows 2008
 - Mouse Settings • 34