



Dominion KSX II

User Guide Release 2.6.0

Copyright © 2014 Raritan, Inc.

DKSXII-v2.6.0-01-E

April 2014

255-62-4030-00

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 2014 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、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan 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.



In Raritan products that require Rack Mounting, please follow these precautions:

- Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the appliances. See **Specifications** (on page 274) in online help.
- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly, especially supply connections, such as power strips (other than direct connections), to the branch circuit.

Contents

Chapter 1 Introduction	1
KSX II Overview	2
What's New in Help	4
Package Contents	4
KSX II Client Applications	5
Product Photos	5
Product Features	6
Hardware	6
Software	7
KSX II Help	7
Chapter 2 Installation and Configuration	8
Overview	8
Default Login Information	8
Getting Started	8
Step 1: Configure the KVM Target Servers	9
Step 2: Configure Network Firewall Settings	12
Step 3: Connect the Equipment	12
Step 4: Configure the KSX II	17
Step 5: Launching the KSX II Remote Console	21
Step 6: Configuring the Keyboard Language (Optional)	22
Allow Pop-Ups	23
Security Warnings and Validation Messages	23
Java Validation and Access Warning	23
Additional Security Warnings	24
Installing a Certificate	24
Example 1: Import the Certificate into the Browser	25
Example 2: Add the KSX II to Trusted Sites and Import the Certificate	27
Chapter 3 Working with Target Servers	29
Interfaces	29
KSX II Local Console: KSX II Devices	30
KSX II Remote Console Interface	31
Proxy Server Configuration for Use with MPC, VKC and AKC	45
Virtual KVM Client (VKC)	46
About the Virtual KVM Client	47
Virtual KVM Client Java Requirements	47
Connecting to a KVM Target Server	47
Switching Between KVM Target Servers	47
Power Controlling a Target Server	48

Disconnecting KVM Target Servers	48
Choosing USB Profiles	49
Connection Properties	50
Connection Information	52
Keyboard	52
Video Properties	56
Mouse Options.....	60
Smart Cards.....	64
Tool Options	67
View Options.....	72
Version Information - Virtual KVM Client	73
Active KVM Client (AKC)	73
Overview	74
Connect to a Target Server	74
AKC Supported Microsoft .NET Framework.....	74
AKC Supported Operating Systems	75
AKC Supported Browsers.....	75
Prerequisites for Using AKC	75
Multi-Platform Client (MPC)	76
Launching MPC from a Web Browser	76
Launching MPC on Mac Lion Clients	77
Raritan Serial Console (RSC).....	78
Opening RSC from the Remote Console	78

Chapter 4 Rack PDU (Power Strip) Outlet Control 80

Overview	80
Turning Outlets On/Off and Cycling Power	81

Chapter 5 Virtual Media 83

Prerequisites for Using Virtual Media	83
KSX II Virtual Media Prerequisites	83
Remote PC VM Prerequisites.....	84
Target Server VM Prerequisites	84
CIMs Required for Virtual Media	84
Mounting Local Drives	84
Notes on Mounting Local Drives.....	84
Supported Tasks Via Virtual Media	85
Supported Virtual Media Types	85
Conditions when Read/Write is Not Available	85
Supported Virtual Media Operating Systems	86
Number of Supported Virtual Media Drives	86
Connecting and Disconnecting from Virtual Media.....	87
Access a Virtual Media Drive on a Client Computer	87
Mounting CD-ROM/DVD-ROM/ISO Images.....	88
Disconnect from Virtual Media Drives	89
Virtual Media in a Windows XP Environment	89
Virtual Media in a Linux Environment	89
Active System Partitions.....	89

Drive Partitions	90
Root User Permission Requirement	90
Virtual Media in a Mac Environment	90
Active System Partition	90
Drive Partitions	90
Virtual Media File Server Setup (File Server ISO Images Only)	91

Chapter 6 USB Profiles 92

Overview	92
CIM Compatibility	93
Available USB Profiles	93
Mouse Modes when Using the Mac Boot Menu	99
Selecting Profiles for a KVM Port	99

Chapter 7 User Management 100

User Groups	100
User Group List	101
Relationship Between Users and Groups	101
Adding a New User Group	101
Modifying an Existing User Group	106
Users	107
Adding a New User	107
View KSX II User List	108
View Users by Port	109
Disconnecting Users from Ports	109
Logging Users Off the KSX II (Force Logoff)	110
Modifying an Existing User	110
Authentication Settings	111
Implementing LDAP/LDAPS Remote Authentication	112
Returning User Group Information from Active Directory Server	115
Implementing RADIUS Remote Authentication	116
Returning User Group Information via RADIUS	120
RADIUS Communication Exchange Specifications	120
User Authentication Process	122
Changing a Password	123

Chapter 8 Device Management 124

Network Settings	124
Network Basic Settings	125
Assign the KSX II an IP Address	125
Configure the IPv4 Settings	125
Configure the IPv6 Settings	126
Configure the DNS Settings	127
LAN Interface Settings	127
Configuring Ports	128
Access the Port Configuration Page	128
Port Configuration Page	129

Configuring KVM Switches	131
Configuring CIM Ports	132
Power Control	134
Configuring Blade Chassis	137
Configuring USB Profiles (Port Page)	158
Configuring KSX II Local Port Settings.....	160
Device Services	163
Enabling Telnet.....	163
Enabling SSH	163
HTTP and HTTPS Port Settings	164
Entering the Discovery Port.....	164
Enabling Serial Console Access.....	164
Enabling Direct Port Access via URL	165
Configuring Direct Port Access via Telnet, IP Address or SSH	167
Enabling the AKC Download Server Certificate Validation	170
Configuring SNMP Agents.....	171
Configuring Modem Settings	173
Configuring Date/Time Settings	174
Event Management.....	175
Configuring Event Management - Settings.....	175
Configuring SNMP Traps.....	176
List of KSX II SNMP Traps	178
Viewing the KSX II MIB	181
SysLog Configuration	182
Configuring Event Management - Destinations.....	182
Connect and Disconnect Scripts.....	183
Applying and Removing Scripts.....	184
Adding Scripts.....	184
Modifying Scripts	187
Importing and Exporting Scripts	187
Port Keywords.....	189
Port Group Management	191
Creating Port Groups.....	191
Changing the Default GUI Language Setting	192

Chapter 9 Security Management 193

Security Settings	193
Login Limitations.....	194
Strong Passwords.....	196
User Blocking.....	197
Encryption & Share.....	199
Enabling FIPS 140-2	202

Configuring IP Access Control	204
SSL Certificates	206
Security Banner	209

Chapter 10 Maintenance 211

Maintenance Features (Local/Remote Console)	211
Audit Log	212
Device Information	213
Backup and Restore	214
USB Profile Management	216
Handling Conflicts in Profile Names	217
Upgrading CIMs	217
Upgrading Firmware	217
Upgrade History	220
Rebooting the KSX II	220
CC Unmanage	221
Stopping CC-SG Management	222

Chapter 11 Diagnostics 224

Network Interface Page	224
Network Statistics Page	224
Ping Host Page	226
Trace Route to Host Page	227
Device Diagnostics	228

Chapter 12 Command Line Interface (CLI) 230

Overview	231
Accessing the KSX II Using CLI	232
SSH Connection to the KSX II	232
SSH Access from a Windows PC	232
SSH Access from a UNIX/Linux Workstation	232
Telnet Connection to the KSX II	233
Enabling Telnet	233
Accessing Telnet from a Windows PC	233
Local Serial Port Connection to the KSX II	233
Port Settings	234
Logging On	234
Navigation of the CLI	236
Completion of Commands	236
CLI Syntax -Tips and Shortcuts	237
Common Commands for All Command Line Interface Levels	237
Initial Configuration Using CLI	238
Setting Parameters	238
Setting Network Parameters	238
CLI Prompts	239
CLI Commands	239
Security Issues	240

Target Connections and the CLI	240
Setting Emulation on a Target	240
Port Sharing Using CLI	241
Administering the KSX II Console Server Configuration Commands	241
Configuring Network	241
Interface Command	242
Name Command	242
Connect Commands	243
IPv6 Command	244

Chapter 13 KSX II Local Console 245

Overview	245
Using the KSX II Local Console	245
Simultaneous Users	245
KSX II Local Console Interface	246
Security and Authentication	246
Available Resolutions	247
Port Access Page (Local Console Server Display)	247
Accessing a Target Server	247
Scanning Ports - Local Console	248
Local Port Scan Mode	249
Local Console Smart Card Access	249
Local Console USB Profile Options	250
Server Display	251
Hot Keys and Connect Keys	252
Connect Key Examples	252
KSX II Supported Keyboard Languages	254
Special Sun Key Combinations	255
Returning to the KSX II Local Console Interface	255
Local Port Administration	256
KSX II Local Console Local Port Settings	256
KSX II Local Console Factory Reset	259
Resetting the KSX II Using the Reset Button	260

Chapter 14 Modem Configuration 261

Certified Modems for UNIX, Linux and MPC	261
Low Bandwidth KVM Settings	262
Client Dial-Up Networking Configuration	263
Windows 2000 Dial-Up Networking Configuration	263
Windows Vista Dial-Up Networking Configuration	267
Windows XP Dial-Up Networking Configuration	268

Appendix A Specifications 274

Hardware	274
KSX II Dimensions and Physical Specifications	274
KSX II Environmental Requirements - KSX II	274
KSX II Electrical Specifications	275

KVM Properties.....	275
Supported Target Server Video Resolution/Refresh Rate/Connection Distance	275
Supported Computer Interface Module (CIMs) Specifications	276
Digital CIM Target Server Timing and Video Resolution.....	278
Digital Video CIMs for Macs	281
Supported Paragon II CIMS and Configurations	282
Supported Remote Connections	285
Network Speed Settings	286
Supported Distances for Serial Devices	287
Connectivity	287
Emergency Connectivity	288
TCP and UDP Ports Used	288
Smart Card Minimum System Requirements	290
Supported and Unsupported Smart Card Readers	292
Mac Mini BIOS Keystroke Commands	293
Using a Windows Keyboard to Access Mac Targets.....	294
KSX II Serial RJ-45 Pinouts.....	294
Software	297
Supported Operating Systems (Clients)	297
Supported Browsers	298
Supported Video Resolutions	299
KSX II Supported Keyboard Languages	301

Appendix B Updating the LDAP/LDAPS Schema 303

Returning User Group Information.....	303
From LDAP/LDAPS	303
From Microsoft Active Directory	303
Setting the Registry to Permit Write Operations to the Schema	304
Creating a New Attribute	304
Adding Attributes to the Class	305
Updating the Schema Cache	307
Editing rcusergroup Attributes for User Members.....	307

Appendix C Informational Notes 311

Overview	311
Java Runtime Environment (JRE) Notes	311
AES 256 Prerequisites and Supported Configurations for Java	311
Java Runtime Environment (JRE)	312
Java Not Loading Properly on Mac	313
IPv6 Support Notes.....	314
Operating System IPv6 Support Notes	314
AKC Download Server Certification Validation IPv6 Support Notes	314
Dell Chassis Cable Lengths and Video Resolutions	315
CIM Notes	315
Windows 3-Button Mouse on Linux Targets.....	315
Smart Card Reader Not Detected when Using a DVM-DP CIM	315
Virtual Media Notes.....	315
Dell OptiPlex and Dimension Computers	315

Contents

Accessing Virtual Media on a Windows 2000	315
Virtual Media Not Refreshed After Files Added.....	316
Target BIOS Boot Time with Virtual Media.....	316
Virtual Media Connection Failures Using High Speed for Virtual Media Connections....	316
USB Port and Profile Notes	316
VM-CIMs and DL360 USB Ports	316
Help Choosing USB Profiles.....	317
Changing a USB Profile when Using a Smart Card Reader	319
Keyboard Notes	319
Non-US Keyboards.....	319
Mac Keyboard Keys Not Supported for Remote Access.....	322
CC-SG Notes	323
Virtual KVM Client Version Not Known from CC-SG Proxy Mode	323
Single Mouse Mode when Connecting to a Target Under CC-SG Control	323
Moving Between Ports on a Device.....	323
Browser Notes	323
Resolving Fedora Core Focus.....	323
Mouse Pointer Synchronization (Fedora)	324
Resolving Issues with Firefox Freezing when Using Fedora	324
VKC and MPC Smart Card Connections to Fedora Servers	324
SUSE/VESA Video Modes	324

Appendix D KSX II FAQs	325
-------------------------------	------------

FAQs.....	325
-----------	-----

Index	339
--------------	------------

Chapter 1 Introduction

In This Chapter

KSX II Overview	2
What's New in Help	4
Package Contents	4
KSX II Client Applications.....	5
Product Photos	5
Product Features	6
KSX II Help	7

KSX II Overview

Raritan's Dominion KSX II is an enterprise-class, secure digital device that provides a single integrated solution for remote KVM (keyboard, video, mouse) server access and serial device management, as well as power control from anywhere in the world from a web browser. At the rack, the KSX II provides control of all KVM server and serial targets from a single keyboard, monitor, and mouse. Total access and control of all serial targets is also available from a single local serial port. The integrated remote access capabilities of the KSX II provide full access and control of your servers from a web browser, or an iPad or iPhone under CC-SG management.

A scan feature allows you to locate and view up to 8 targets. The targets are displayed as thumbnails in a slide show from which users connect to each target.

KSX II is easily installed using standard UTP (Cat 5/5e/6) cabling. Its advanced features include virtual media, up to 256-bit encryption, remote power control, dual Ethernet, LDAP, RADIUS, Active Directory®, Syslog integration, and web management. These features enable you to deliver higher uptime, better productivity, and bulletproof security - any time from anywhere.

KSX II products can operate as standalone devices and do not rely on a central management device. For larger data centers and enterprises, multiple KSX II devices can be integrated into a single logical solution with other Raritan devices using Raritan's CommandCenter Secure Gateway (CC-SG) management unit.

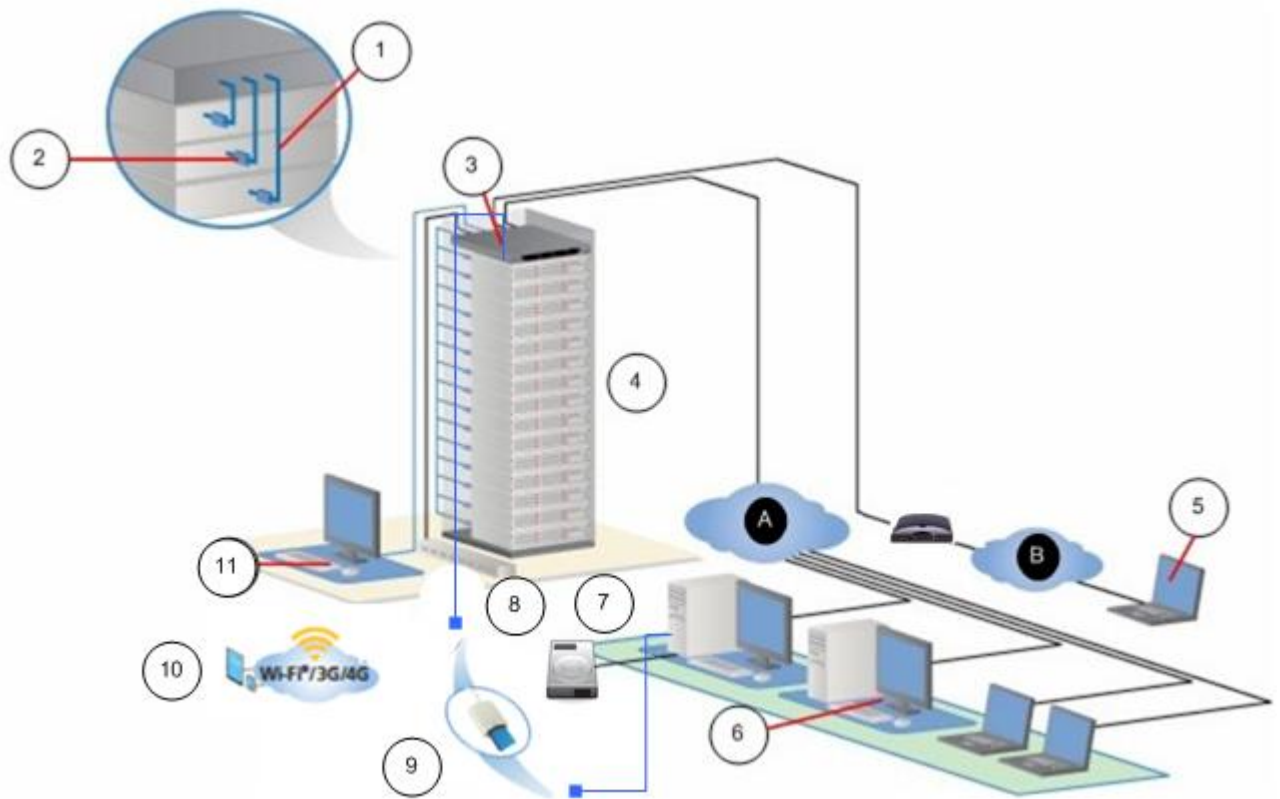


Diagram key

1	Cat5 cable	8	Rack PDU (power strip)
2	Computer Interface Module (CIM)	9	Local and remote smart card access
3	KSX II	10	Mobile access via iPhone® and iPad® using CC-SG
4	Remote KVM and serial devices	11	Local access
5	Modem access	A	IP LAN/WAN
6	Remote (network) access	B	PSTN
7	Remote virtual media USB drive(s)		

What's New in Help

The following information has been added based on enhancements and changes to the equipment and/or user documentation.

- Support Internet Explorer® 11
- Requirement to use Java™ 1.7
- Recommendation to install an SSL certificate in order to avoid Java warnings. See ***Installing a Certificate*** (on page 24)
- Use of an NTP server when DHCP is enabled. See ***Network Settings*** (on page 124)
- Ability to apply the native resolution of a CIM to other CIMs of the same type. See ***Apply a Native Display Resolution to Other CIMs*** (on page 134)
- Enable and disable Favorites in the KSX II Remote Client - see ***Managing Favorites*** (on page 39)

Please see the KSX II Release Notes for a more detailed explanation of the changes applied to the appliance and this version of the help.

Package Contents

Each KSX II ships as a fully-configured stand-alone product in a standard 1U 19" rackmount chassis.

Each KSX II device ships with the following contents:

- 1 - Dominion KSX II device
 - 1 - Quick Setup Guide
 - 1 - Rackmount kit
 - 1 - AC power cord
 - 1 - Cat5 network cable
 - 1 - Cat5 network crossover cable
 - 1 - Set of 4 rubber feet (for desktop use)
 - 1 - Application notes
 - 1 - Warranty card
 - 1 - Phone line cable
- 1 - Loopback adapter

KSX II Client Applications

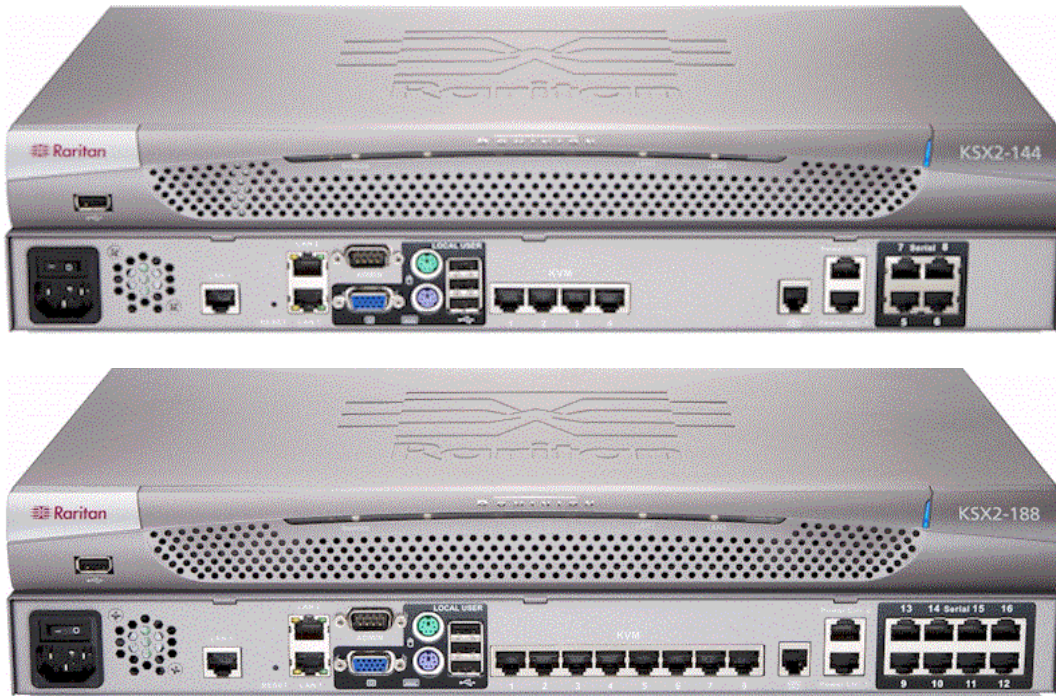
The following client applications can be used with the KSX II:

- Virtual KVM Client (VKC)
- Active KVM Client (AKC)
- Multiplatform Client (MPC)
- Raritan Serial Console (RSC)

Java™ 1.7 is required to use the Java-based KSX II Virtual KVM Client (VKC) and Multi-Platform Client (MPC)..

Microsoft .NET® 3.5 (or later) is required to use KSX II with the Microsoft Windows®-based Active KVM Client (AKC).

Product Photos



Product Features

Hardware

- KVM and serial remote access over IP
- 1U rack-mountable; brackets included
- DKSX2-144 - 4 serial/4 KVM server ports
- DKSX2-188 - 8 serial/8 KVM server ports
- 1 KVM channel shareable by 8 users, multiple serial users.
- UTP (Cat5/5e/6) server cabling
- Dual Ethernet ports (10/100/1000 LAN) with failover
- Field upgradeable
- Local KVM port for in-rack access
 - Keyboard/mouse ports
 - One front and three back panel USB 2.0 ports for supported USB devices
 - Fully concurrent with remote user access
 - Local Graphical User Interface (GUI) for administration
 - Both KVM and serial targets can be connected using KVM local port
- Local serial port (RS232) for CLI-based administration and serial target access
- Integrated power control
- Dual dedicated power control ports
- LED indicators for network activity, and remote KVM user status
- Hardware reset button
- Internal modem
- Centralized access security

Software

- Virtual media support in Windows®, Mac® and Linux® environments with D2CIM-VUSB and D2CIM-DVUSB CIMs and digital CIMs
- Port scanning and thumbnail view of up to 8 targets within a configurable scan set
- Absolute Mouse Synchronization with D2CIM-VUSB CIM, D2CIM-DVUSB CIM and digital CIMs
- Plug-and-Play
- Web-based access and management
- Intuitive Graphical User Interface (GUI)
- 256-bit encryption of complete KVM signal, including video and virtual media
- LDAP/LDAPS, Active Directory®, RADIUS, or internal with local authentication and authorization
- DHCP or fixed IP addressing
- Smart card/CAC authentication
- SNMP 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 the device from CC-SG control

KSX II Help

KSX II online help is considered your primary help resource. PDF versions of help are a secondary resource.

See the KSX II Release Notes for important information on the current release before you begin using the KSX II.

KVM Client help is provided as part of KSX II online help.

Online help is accompanied by the KSX II Quick Setup Guide, which is included with your KSX II and can be found on the Raritan Support page of **Raritan's website** (<http://www.raritan.com/support/firmware-and-documentation>).

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

Chapter 2 Installation and Configuration

In This Chapter

Overview	8
Default Login Information	8
Getting Started	8
Allow Pop-Ups	23
Security Warnings and Validation Messages	23
Installing a Certificate	24

Overview

This section provides a brief overview of the installation process. Each step is further detailed in the remaining sections of this chapter.

Before installing the KSX II, configure the target server you want to access via the KSX II so you ensure optimum performance.

Default Login Information

Default	Value
User name	<i>admin</i> This user has administrative privileges.
Password	<i>raritan</i> The first time you start the KSX II, you are required to change the default password.
IP address	192.168.0.192.
Important: For backup and business continuity purposes, it is strongly recommended that you create a backup administrator user name and password and keep that information in a secure location.	

Getting Started

Note that the following configuration requirements apply only to the target server, not to the computers that you remotely access the KSX II.

Step 1: Configure the KVM Target Servers

For optimal bandwidth efficiency and video performance, KVM target servers running graphical user interfaces such as Windows®, Linux®, X-Windows, Solaris™, and KDE may require configuration.

The desktop background does not need to be completely solid, but desktop backgrounds featuring photos or complex gradients might degrade performance.

Target Server Video Resolutions

For optimal bandwidth efficiency and video performance, KVM target servers running graphical user interfaces such as Windows®, Linux®, X-Windows, Solaris™, and KDE may require configuration.

The desktop background does not need to be completely solid, but desktop backgrounds featuring photos or complex gradients might degrade performance.

Ensure that the server video resolution and refresh rate are supported by KSX II and that the signal is non-interlaced.

See the **KSX II Online Help** for a list of supported target server video resolutions.

Mouse Settings

Following are the mouse settings for various operating systems.

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

See the **KSX II Online Help** for details on configuring these mouse settings.

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.

Once you have completed your KSX II 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 KSX II, 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 2: Configure Network Firewall Settings

TCP Port 5000

Allow network and firewall communication on TCP Port 5000 to enable remote access to the KSX II.

Alternatively, configure the KSX II to use a different TCP port, then allow communication on that port.

TCP Port 443

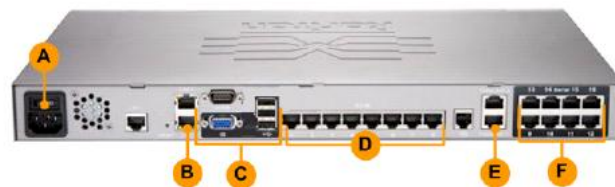
Allow access to TCP Port 443 (Standard HTTPS) so you can access KSX II via a web browser.

TCP Port 80

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

Step 3: Connect the Equipment

Connect the KSX II to the power supply, network, local PC, local video display, keyboard and mouse, KVM target servers, and serial targets.



A. AC Power

► **To connect the power supply:**

1. Attach the included AC power cord to the KSX II and plug into an AC power outlet.

B. Network Port

The KSX II provides two Ethernet ports for failover purposes (not for load-balancing). By default, only LAN1 is active and the automatic failover is disabled. When enabled, if the KSX II internal network interface or the network switch to which it is connected becomes unavailable, LAN2 will be enabled using the same IP address.

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

► To connect the network:

1. Connect a standard Ethernet cable (included) from the network port labeled LAN1 to an Ethernet switch, hub, or router.
2. To make use of the optional KSX II Ethernet failover capabilities:
 - Connect a standard Ethernet cable from the network port labeled LAN2 to an Ethernet switch, hub, or router.
 - Enable Automatic Failover on the Network Configuration page.

Note: Use both network ports only if you want to use one as a failover port.

C. Local User Port (Local PC) and Local Admin Port

For convenient access to KVM target servers and serial devices while at the rack, use the KSX II Local Access port. While the local port is required for installation and setup, it is optional for subsequent use. The local port provides the KSX II Local Console graphical user interface for administration and target server access.

► To connect the Local User port:

- Attach a multi-sync VGA monitor, keyboard, and mouse to the respective Local User ports using a USB keyboard and mouse.
- Monitor - Attach a standard multi-sync VGA monitor to the HD15 (female) video port
- Keyboard - Attach either a standard keyboard to the Mini-DIN6 (female) keyboard port, or a standard USB keyboard to one of the USB Type A (female) ports
- Mouse - Attach either a standard mouse to the Mini-DIN6 (female) mouse port or a standard USB mouse to one of the USB Type A (female) ports

You can use the Local Admin port to connect the KSX II directly to a workstation to manage your serial targets and configure the system with a terminal emulation program such as HyperTerminal. The Local Admin port requires the use of a standard null modem cable.

Note: When local Authorization and Authentication is set to None, logging in to serial admin console requires username input.

D. KVM Target Server Ports

The KSX II uses standard UTP cabling (Cat5/5e/6) to connect to each target server.

► To connect a KVM target server to the KSX II:

1. Use the appropriate Computer Interface Module (CIM).
2. Attach the HD15 video connector of your CIM to the video port of your KVM target server. Ensure that your target server's video has already been configured to a supported resolution and refresh rate. For Sun servers, also ensure that your target server's video card has been set to output standard VGA (H-and-V sync) and not composite sync.
3. Attach the keyboard/mouse connector of your CIM to the corresponding ports on your target server. Using a standard straight-through UTP (Cat5/5e/6) cable, connect the CIM to an available server port on the back of your KSX II device.

Note: The DCIM-USB G2 provides a small slide switch on the back of the CIM. Move the switch to P for PC-based USB target servers. Move the switch to S for Sun USB target servers. Power-cycle the CIM by removing the USB connector from the target server, then plugging it back in a few seconds later in order to apply the new switch position.

E. Power Strip

► To connect the Dominion PX to the KSX II:

1. Plug one end of a Cat5 cable into the Serial port on the front of the Dominion PX.
2. Connect the other end of the Cat5 cable to either the Power Ctrl. 1 or Power Ctrl. 2 ports on the back of the KSX II.
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 KSX II device.

Important: When using CC-SG, the power ports should be inactive before attaching rack PDUs that were swapped between the power ports. If this is not done, there is a possibility that the number of power outlets will not be correctly detected, especially after swapping 8 and 20 outlet rack PDU models.

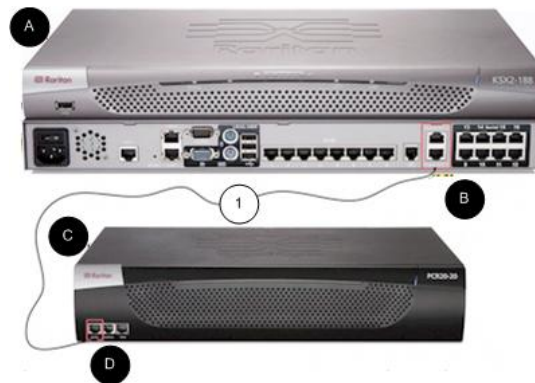







Diagram key			
	KSX II		PX serial port
	KSX II Power Ctrl. 1 Port or Power Ctrl. 2 Port		Cat5 cable
	PX		

F. Serial Target Ports

To connect a serial target to the KSX II, use a Cat5 cable with an appropriate serial adapter.

The following table lists the necessary KSX II hardware (adapters and/or cables) for connecting the KSX II to common vendor/model combinations.

Vendor	Device	Console connector	Serial connection
Checkpoint	Firewall	DB9M	ASCSD9F adapter and a CAT 5 cable
Cisco	PIX Firewall		
Cisco	Catalyst	RJ-45	CRLVR-15 rollover cable; or CRLVR-1 adapter cable and a CAT5 cable CRLVR-1 cable for connecting a terminal port (RJ-45 Connector type) of KSX II-48 models that have this connector to another KSX II.
Cisco	Router	DB25F	ASCSD25M adapter and a CAT 5 cable
Hewlett Packard®	UNIX® Server	DB9M	ASCSD9F adapter and a

Vendor	Device	Console connector	Serial connection
Silicon Graphics	Origin		CAT 5 cable
Sun™	SPARCStation	DB25F	ASCSD25M adapter and a CAT 5 cable
Sun	Netra T1	RJ-45	CRLVR-15 cable; or CRLVR-1 adapter and a CAT5 cable
Sun	Cobalt	DB9M	ASCSD9F adapter and a CAT 5 cable
Various	Windows NT®		

Go to the Support page on Raritan's website (www.raritan.com) to obtain a list of commonly used cables and adapters.

Step 4: Configure the KSX II

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

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

Java™ 1.7 is required to use the Java-based KSX II Virtual KVM Client (VKC) and Multi-Platform Client (MPC)..

Microsoft .NET® 3.5 (or later) is required to use KSX II with the Microsoft Windows®-based Active KVM Client (AKC).

Change the Default Password

The first time you start the KSX II, you are required to change the default password.

► To change the default password:

1. Once the unit has booted, enter the default username *admin* and password *raritan*. Click Login.
2. Enter the old password *raritan*, then enter and reenter a new password.

Passwords can be up to 64 characters in length consisting of English, alphanumeric and special characters.

3. Click Apply. Click OK on the Confirmation page.

Assign the KSX II an IP Address

► To assign an IP address to the KSX II:

1. Choose Device Settings > Network. The Network Settings page opens.
2. Specify a meaningful Device Name for your KSX II device.
Up to 32 alphanumeric and valid special characters, no spaces between characters.
3. Next, configure the IPv4, IPv6 and DNS settings.

Configure the IPv4 Settings

1. In the IPv4 section, enter or select the appropriate IPv4-specific network settings:
 - a. Enter the IP Address if needed. The default IP address is 192.168.0.192.
 - b. Enter the Subnet Mask. The default subnet mask is 255.255.255.0.
 - c. Enter the Default Gateway if None is selected from the IP Auto Configuration drop-down.
 - d. Enter the Preferred DHCP Host Name if DHCP is selected from the IP Auto Configuration drop-down.
 - e. Select the IP Auto Configuration. The following options are available:
 - None (Static IP) - This option requires you manually specify the network parameters.

This is the recommended option because the KSX II is an infrastructure device, and its IP address should not change.

Select this option if you want to ensure redundant failover capabilities should the primary Ethernet port (or the switch/router to which it is connected) fail. If it fails, KSX II fails over to the secondary network port with the same IP address, ensuring there is not interruption.
 - DHCP - Dynamic Host Configuration Protocol is used by networked computers (clients) to obtain unique IP addresses and other parameters from a DHCP server.

With this option, network parameters are assigned by the DHCP server.

If DHCP is used, enter the Preferred host name (DHCP only). Up to 63 characters.
2. Next, configure IPv6 and/or DNS settings.

Configure the IPv6 Settings

1. If using IPv6, enter or select the appropriate IPv6-specific network settings in the IPv6 section:
 - a. Select the IPv6 checkbox to activate the fields in the section and enable IPv6 on the device.
 - b. Enter a Global/Unique IP Address. This is the IP address assigned to the KSX II.
 - c. Enter the Prefix Length. This is the number of bits used in the IPv6 address.
 - d. Enter the Gateway IP Address.
 - e. Link-Local IP Address. This address is automatically assigned to the device, and is used for neighbor discovery or when no routers are present. **Read-Only**
 - f. Zone ID. Identifies the device the address is associated with. **Read-Only**
 - g. Select an IP Auto Configuration option:
 - None (Static IP) - this option requires you manually specify the network parameters.

This is the recommended option because the KSX II is an infrastructure device, and its IP address should not change.

Select this option if you want to ensure redundant failover capabilities should the primary Ethernet port (or the switch/router to which it is connected) fail. If it fails, KSX II switches to the secondary network port with the same IP address, ensuring there is no interruption.

If None is selected, the following Network Basic Settings fields are enabled: Global/Unique IP Address, Prefix Length, and Gateway IP Address allowing you to manually set the IP configuration.
 - Router Discovery - use this option to automatically assign IPv6 addresses that have Global or Unique Local significance beyond that of the Link Local, which only applies to a directly connected subnet.
2. Next, configure DNS settings.

Configure the DNS Settings

1. Select Obtain DNS Server Address Automatically if DHCP is selected and Obtain DNS Server Address is enabled. When Obtain DNS Server Address Automatically, the DNS information provided by the DHCP server will be used.

2. If Use the Following DNS Server Addresses is selected, whether or not DHCP is selected, the addresses entered in this section is used to connect to the DNS server.

Enter the following information if the Following DNS Server Addresses is selected. These addresses are the primary and secondary DNS addresses used if the primary DNS server connection is lost due to an outage.

- a. Primary DNS Server IP Address
 - b. Secondary DNS Server IP Address
3. When finished, click OK.

Your KSX II device is now network accessible.

Name Your Target Servers

► To name the target servers:

1. Connect all of the target servers if you have not already done so.
2. Select Device Settings > Port Configuration, then click the Port Name of the target server you want to name.
3. Enter a name for the server up to 32 alphanumeric and special characters. Click OK.

Configure Date/Time Settings (Optional)

Optionally, configure the date and time settings.

The date and time settings impact SSL certificate validation if LDAPS is enabled.

Use the Date/Time Settings page to specify the date and time for the KSX II. 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.

Step 5: Launching the KSX II Remote Console

Log in to your KSX II Remote Console from any workstation with network connectivity that has Microsoft .NET® and/or Java Runtime Environment™ installed.

► To launch the KSX II Remote Console:

1. Launch a supported web browser.
2. Enter either:
 - The URL - `http://IP-ADDRESS` to use the Java-based Virtual KVM Client

Or

 - `http://IP-ADDRESS/akc` for the Microsoft .NET-based Active KVM Client

IP-ADDRESS is the IP address assigned to your KSX II

You can also use HTTPS, or the DNS name of the KSX II assigned by your administrator (if applicable).

3. You are always redirected to the IP address from HTTP to HTTPS.
4. Enter your username and password. Click Login.

Access and Control Target Servers Remotely

The KSX II Port Access page provides a list of all KSX II ports, as well as the connected target servers, their status, and availability.

Accessing a Target Server

► **To access a target server:**

1. On the KSX II 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.

Switching between Target Servers

► **To switch between KVM target servers:**

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

Disconnecting a Target Server

► **To disconnect a target server:**

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

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.

Changing 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.

Allow Pop-Ups

Regardless of the browser used, you must allow pop-ups from the device's IP address to launch the KSX II Remote Console.

Security Warnings and Validation Messages

When logging in to KSX II, security warnings and application validation message may appear.

These include:

- Java™ security warnings and requests to validate KSX II. See **Java Validation and Access Warning** (on page 23), and **Installing a Certificate** (on page 24)
- Additional security warnings based on your browser and security settings. See **Additional Security Warnings** (on page 24)

Java Validation and Access Warning

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

Raritan recommends installing an SSL certificate in each KSX II device in order to reduce Java warnings, and enhance security. See **SSL Certificates** (on page 206)

Additional Security Warnings

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

It is necessary to accept these warnings to launch the KSX II 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 KSX II's SSL certificate.

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

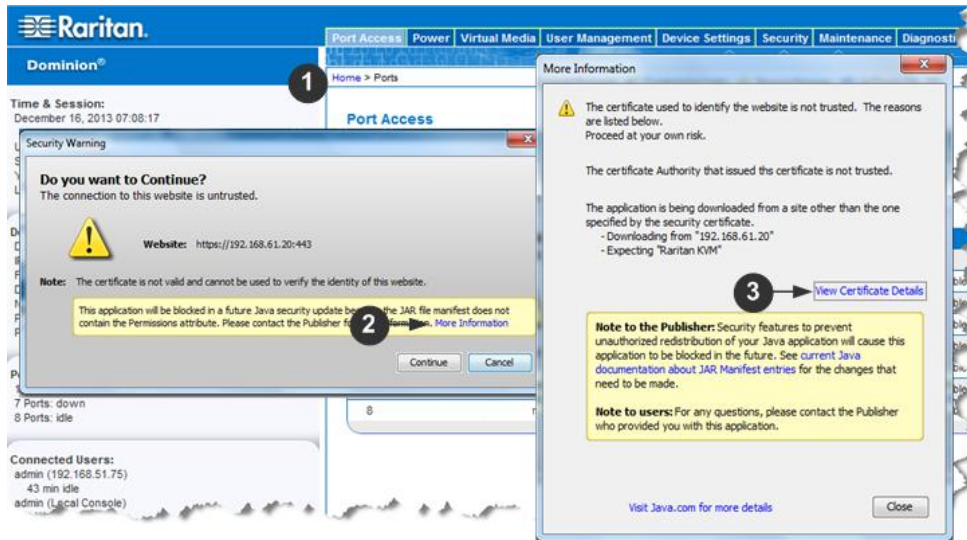
It is necessary to accept these warnings to launch the KSX II Remote Console. For more information, see ***Security Warnings and Validation Messages*** (on page 23).

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.

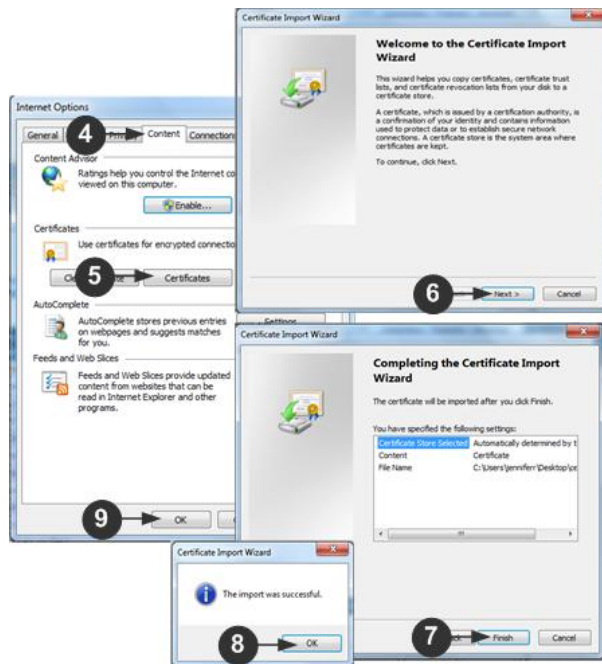
Example 1: Import the Certificate into the Browser

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



Steps

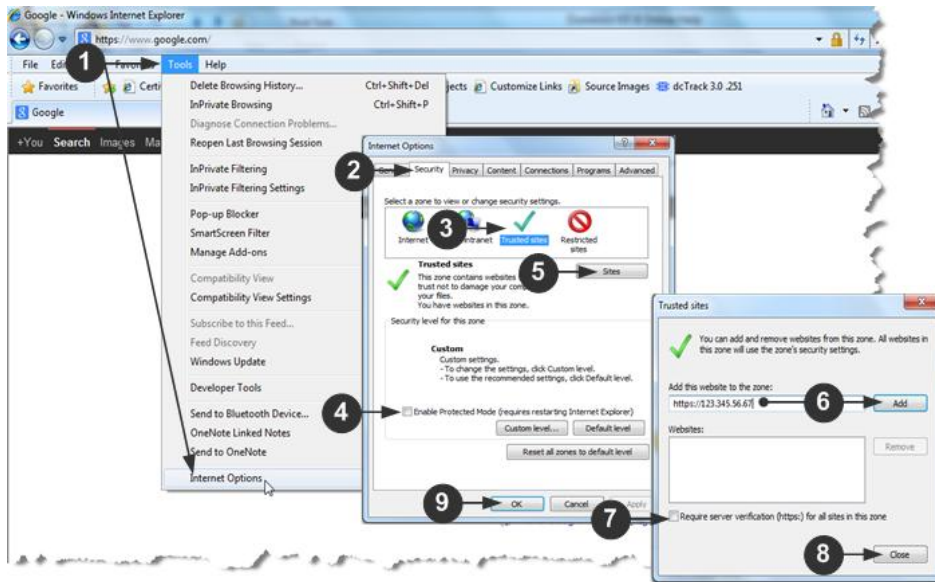
1	Open an IE browser, then log in to KSX II.
2	Click More Information on the first Java™ security warning.
3	Click View Certificate Details on the More Information dialog. You are prompted to install the certificate. Follow the wizard steps.
<p><i>Note: If you are not prompted by the browser, manually select Tools > Internet Options to open the Internet Options dialog.</i></p>	



Steps	
4	Click the Content tab.
5	Click Certificates.
6	The Certificate Import Wizard opens and walks you through each step. <ul style="list-style-type: none"> File to Import - Browse to locate the Certificate Certificate Store - Select the location to store the Certificate
7	Click Finish on the last step of the Wizard.
8	The Certificate is imported. Close the success message.
9	Click OK on the Internet Options dialog to apply the changes, then close and reopen the browser.

Example 2: Add the KSX II to Trusted Sites and Import the Certificate

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

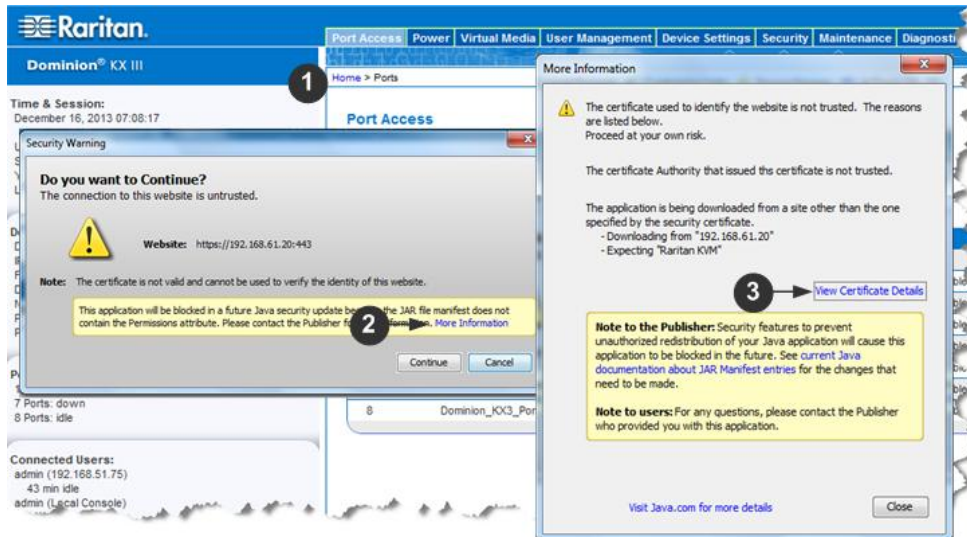


Steps

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 KSX II URL, then click Add.
7	Deselect server verification for the zone (if applicable).
8	Click Close.

Steps

- 9 Click OK on the Internet Options dialog to apply the changes, then close and reopen the browser.
Next, import the Certificate.



Steps

- 1 Open an IE browser, then log in to KSX II.
- 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 25)

Chapter 3 Working with Target Servers

In This Chapter

Interfaces	29
Proxy Server Configuration for Use with MPC, VKC and AKC	45
Virtual KVM Client (VKC).....	46
Active KVM Client (AKC)	73
Multi-Platform Client (MPC).....	76
Raritan Serial Console (RSC).....	78

Interfaces

There are several interfaces in the KSX II providing you with easy access any time, anywhere. The following table identifies these interfaces and their use of target server access and administration locally and remotely:

User interface	Local		Remote	
	Access	Admin	Access	Admin
KSX II Local Console	✓	✓		
KSX II Remote Console			✓	✓
Virtual KVM Client (VKC)			✓	
Active KVM Client (AKC)			✓	✓
Multi-Platform Client (MPC)			✓	✓
Raritan Serial Console (RSC)			✓	
Command Line Interface (CLI)	✓	✓	✓	✓

The following sections of the user guide contain information about using specific interfaces to connect to the KSX II and manage targets:

- ***KSX II Local Console Interface: KSX II Devices*** (see "***KSX II Local Console: KSX II Devices***" on page 30)
- ***KSX II Remote Console Interface*** (on page 31)
- ***Virtual KVM Client (VKC)*** (on page 46)
- ***Active KVM Client (AKC)*** (on page 73)
- ***Multi-Platform Client (MPC)*** (on page 76)
- ***Raritan Serial Console (RSC)*** (on page 78)
- ***Command Line Interface (CLI)*** (on page 230)

KSX II Local Console: KSX II Devices

When you are located at the server rack, the KSX II provides standard KVM management and administration via the KSX II Local Console. The KSX II Local Console provides a direct KVM (analog) connection to your connected servers; the performance is exactly as if you were directly connected to the server's keyboard, mouse, and video ports. Additionally, the KSX II provides terminal emulation when accessing serial targets.

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

KSX II Remote Console Interface

The KSX II 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 KSX II and to remotely administer the KSX II.

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

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

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

Note: If you are using Internet Explorer® 7, you may run into permission issues when trying to connect to a target server. To avoid this, do the following:

- 1. In Internet Explorer, click Tools > Internet Options to open the Internet Options dialog.*
 - 2. In the "Temporary Internet files" section, click Settings. The Settings dialog opens.*
 - 3. In the "Check for newer versions of stored pages" section, select Automatically.*
 - 4. Click OK to apply the settings.*
-

Launching the KSX II Remote Console

Important: Regardless of the browser used, you must allow pop-ups from the device's IP address to launch the KSX II Remote Console.

Depending on your browser and security settings, you may see various security and certificate warnings. It is necessary to accept these warnings to launch the KSX II Remote Console.

You can reduce the number of warning messages during subsequent logins 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.

Log in to your KSX II Remote Console from any workstation with network connectivity that has Microsoft .NET® and/or Java Runtime Environment™ installed.

► **To launch the KSX II Remote Console:**

1. Launch a supported web browser.
2. Enter either:
 - The URL - *http://IP-ADDRESS* to use the Java-based Virtual KVM Client

Or

 - *http://IP-ADDRESS/akc* for the Microsoft .NET-based Active KVM Client

IP-ADDRESS is the IP address assigned to your KSX II

You can also use HTTPS, or the DNS name of the KSX II assigned by your administrator (if applicable).

You are always redirected to the IP address from HTTP to HTTPS.

3. Type your user name and password. If this is the first time logging in, log in with the factory default user name (admin) and password (raritan, all lower case). You will be prompted to change the default password. Click Login.

Note: If your administrator requires you read and/or accept a security agreement in order to access the device, a security banner will be displayed after you have entered your login credentials and clicked Login.

See Virtual KVM Client (VKC) and Active KVM Client (AKC) for information on the KSX II functions available via the Remote Console.

Interface and Navigation

KSX II Interface

Both the KSX II Remote Console and the KSX II Local Console interfaces provide a web-based interface for device configuration and administration, as well as target server list and selection. The options are organized into various tabs.

After a successful login, the Port Access page opens listing all ports along with their status and availability. Four tabs are provided on the page allowing you to view by port, view by group or view by search. 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. See Port Access Page (Remote Console Display) for more information.

Use the Set Scan tab to scan for up to 32 targets that are connected to the KSX II. See Scanning Ports.

Left Panel

The left panel of the KSX II 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 KSX II	Always
Last Login	The last login date and time	Always
Under CC-SG Management	The IP address of the CC-SG device managing the KSX II	When the KSX II is being managed by CC-SG.
Device Information	Information specific to the KSX II you are using	Always
Device Name	Name assigned to the device	Always
IP Address	The IP address of the KSX II. If IPv6 is enabled, the IPv6 address will also be listed	Always
Firmware	Current version of firmware	Always
Device Model	Model of the KSX II	Always
Network	The name assigned to the current network LAN1 or LAN2	Always
Port States	The statuses of the ports being used by the KSX II	Always

Information	Description	When displayed?
Connected Users	The users, identified by their username and IP address, who are currently connected to the KSX II	Always
Online Help - User Guide	Links to online help	Always
FIPS Mode	FIPS Mode: EnabledSSL Certificate: FIPS Mode Compliant	When FIPS is enabled
Favorite Devices	See <i>Managing Favorites</i> (on page 39)	When enabled

KSX II Console Navigation

The KSX II Console interfaces provide many methods for navigation and making your selections.

► **To select an option (use any of the following):**

- Click on a tab. A page of available options appears.
- Hover over a tab and select the appropriate option from the menu.
- Click the option directly from the menu hierarchy displayed (breadcrumbs).

► **To scroll through pages longer than the screen:**

- Use Page Up and Page Down keys on your keyboard.
- Use the scroll bar on the right.

Port Access Page (Remote Console Display)

After successfully logging on to the KSX II remote console, the View by Port tab on the Port Access page appears. This page lists all of the KSX II ports, and the target servers, port groups, and blade chassis that are connected to those ports.

The information is sorted by Port Number by default, but you can change the display to sort on any of the available columns by clicking on a column header. To increase or decrease the number of rows displayed on a tab at one time, enter the number of row in the Rows per Page field and click Set.

The following information for each port is contained on this page:

- Port Number - Numbered from 1 to the total number of ports available for the KSX II device.
- Port Name - The name of the KSX II port. Initially, this is set to Dominion_KSX2_Port# but you can change the name to something more descriptive. When you click a Port Name link, the Port Action Menu appears.

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

- Type - The type of server or CIM/DCIM.
For blade chassis, the type can be Blade Chassis, Blade, BladeChassisAdmin, and BladeChassisURL.
- Status - The status of the servers - either up or down.

Home > Ports Logout

Port Access

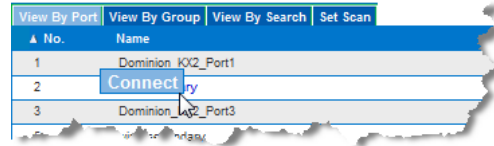
Click on the individual port name to see allowable operations.
0 / 1 Remote KVM channels currently in use.

View By Port	View By Group	View By Search	Set Scan				
▲ No.	Name	Type	Status	Availability			
1	▶ CMC-GSBN6G1	BladeChassis	up	idle			
2	Target-Server	DCIM	up	idle			
3	▼ IBM-H-CHASSIS	BladeChassis	up	idle			
3-1	Blade_Chassis_Port3_Slot1	Blade	-	-			
3-2	Blade_Chassis_Port3_Slot2	Blade	-	-			
3-3	Blade_Chassis_Port3_Slot3	Blade	-	-			
3-4	Blade_Chassis_Port3_Slot4	Blade	-	-			
3-5	Blade_Chassis_Port3_Slot5	Blade	-	-			
3-6	Blade_Chassis_Port3_Slot6	Blade	-	-			
3-7	Blade_Chassis_Port3_Slot7	Blade	-	-			

► **To connect to an available target server:**

1. Click on the port name. The Port Action menu opens.

- Click Connect. Once you are connected to a target or dual monitor target server, click on the port group name and then click Disconnect to disconnect.



See **Port Action Menu** (on page 38) for details on additional available menu options.

► **To change the display sort order and/or view more ports on the same page:**

- Click the column heading by which you want to sort. The list of is sorted by that column.
- In the Rows per Page, enter the number of ports to be displayed on the page and click Set.

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 hierarchal order, blade-chassis subtypes must be configured for the blade server chassis.

View by Group Tab

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

See Device Management for information on creating each of these types of port groups.

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.

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 See Scanning Ports - Remote Console 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 - Creates a new connection to the target server.

For the KSX II Remote Console, a new **Virtual KVM Client** (see "**Virtual KVM Client (VKC)**" on page 46) page appears.

For the KSX II Local Console, the display switches to the target server, and switches away from the local user interface.

On the local port, the KSX II 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 KSX II Remote Console for an available port if all connections are busy.

- 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 KSX II Local Console.

- 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 KSX II Local Console. The only way to disconnect from the switched target in the Local Console is to use the hot key.

- **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.

- **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.

- **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.

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 side (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 KSX II devices on its subnet (before and after login)
- Retrieve discovered KSX II devices from the connected Dominion device (after login)

Enable Favorites

- Click Enable in the Favorite Devices section of the left panel of the KSX II interface.

Once enabled, the Enable button becomes a Disable button.

The screenshot displays the Raritan Dominion web interface. The left sidebar contains several sections: 'Time & Session' (showing date and time), 'User' (showing admin status), 'Device Information' (showing device name, IP, firmware, and model), 'Port States' (showing up/down/idle ports), 'Connected Users' (showing active users), 'Online Help', and 'Favorite Devices'. In the 'Favorite Devices' section, there is an 'Enable' button with a red arrow pointing to it. The main content area on the right shows 'Port Access' and a table of ports with columns 'No.' and 'Name'.

No.	Name
1	Window
2	Low Co
3	DP-Dom
4	WinXP-P
5	Dominio
6	Dominio
7	Dominio
8	Dominio
9	Dominio
10	Dominio
11	Dominio
12	Dominio
13	Dominio
14	Dominio
15	Dominio
16	Dominio
17	Dominio

Access and Display Favorites► **To access a favorite KSX II device:**

- Click the device name (listed beneath Favorite Devices). A new browser opens to that device.

► **To display favorites by name:**

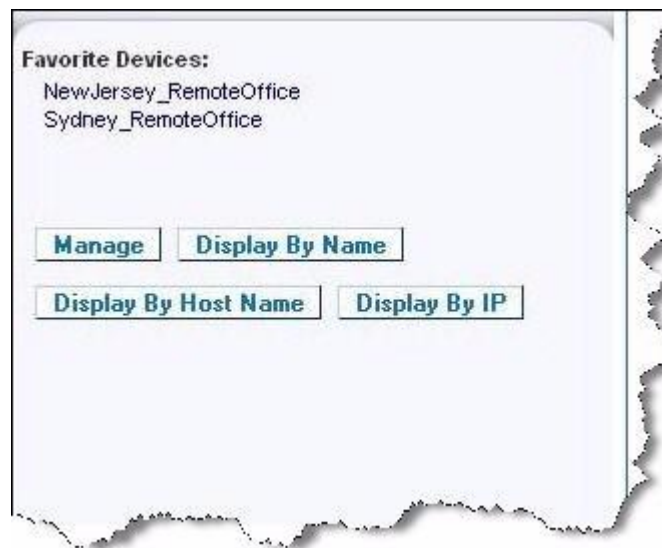
- Click Display by Name.

► **To display favorites by IP Address:**

- Click Display by IP.

► **To display favorites by the host name:**

- Click Display by Host Name.

**Discovering Devices on the Local Subnet**

This option discovers the devices on your local subnet, which is the subnet where the KSX II Remote Console is running. These devices can be accessed directly from this page or you can add them to your list of favorites. See Favorites List Page.

► **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 KSX II Subnet

This option discovers devices on the device subnet, which is the subnet of the KSX II device IP address itself. You can access these devices directly from this the Subnet page or add them to your list of favorites. See Favorites List Page.

This feature allows multiple KSX II devices to interoperate and scale automatically. The KSX II Remote Console automatically discovers the KSX II devices, and any other Raritan device, in the subnet of the KSX II.

► **To discover devices on the device subnet:**

1. Choose Manage > Discover Devices - KSX II Subnet. The Discover Devices - KSX II 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.

Scanning Ports

The KSX II provides a port scanning feature that searches for selected targets and displays them in a slide show view, allowing you to monitor up to 8 targets at one time. You can connect to targets or focus on a specific target as needed.

Scans can include standard targets and blade servers ports. Configure scan settings from either the Virtual KVM Client (VKC) or Active KVM Client (AKC). See **Configure Scan Settings in VKC and AKC** (on page 71) for more information.

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.

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 and AKC

► 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

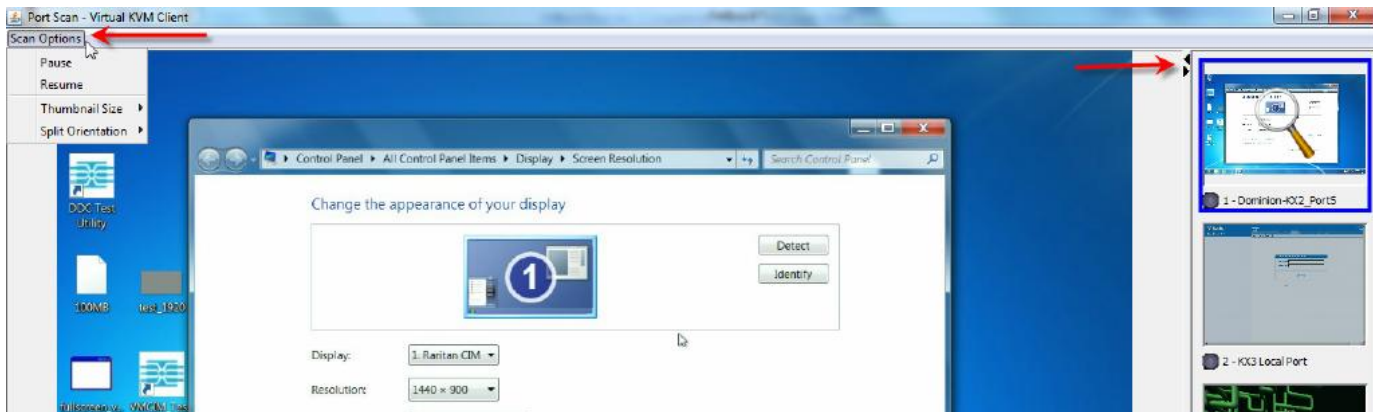
- Resume the thumbnail rotation by selecting Options > Resume.

► 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.



Logging Out

► To quit the KSX II:

- Click Logout in the upper right-hand corner of the page.

Note: Logging out also closes any open Virtual KVM Client and serial client sessions.

Proxy Server Configuration for Use with MPC, VKC 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).

3. If you are using standalone Multi-Platform Client (MPC), you must also do the following:
 - a. Open the start.bat file in MPC directory with a text editor.
 - b. Insert the following parameters to the command line. Add them before "-classpath": -DsocksProxyHost=<socks proxy ip addr> -DsocksProxyPort=<socks proxy port>

The parameters are:

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

Virtual KVM Client (VKC)

Please note this client is used by various Raritan products. As such, references to other products may appear in this section of help.

About the Virtual KVM Client

Whenever you access a target server from the Port Access page of KSX II 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.

Note: Refreshing your HTML browser closes the Virtual KVM Client connection, so exercise caution.

Note: If you are using Firefox 3.0.3, you may experience problems launching the application. If this occurs, clear the browser cache and launch the application again.

Virtual KVM Client Java Requirements

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

Connecting to a KVM Target Server

► **To connect to a KVM target server:**

1. From the KSX II Remote Console, click the Port Access tab to open it. The Port Access page opens.
2. Click the Port Name of the target you want to access. The Port Action menu appears.
3. Click Connect. A Virtual KVM Client window opens to the target server connected to that port.

Switching Between KVM Target Servers

With the KSX II, you can access several KVM target servers. The KSX II provides the ability to switch from one target server to another.

Note: This feature is available in the KSX II Remote Console only.

► **To switch between KVM target servers:**

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

Power Controlling a Target Server

Note: These features are available only when you have made power associations.

► **To power cycle a KVM target server:**

1. From the KSX II Remote Console, click the Port Access tab. The Port Access page opens.
2. Click the Port Name of the appropriate target server. The Port Action menu appears.
3. Choose Power Cycle. A confirmation message appears.

► **To power on a target server:**

1. From the KSX II Remote Console, click the Port Access tab. The Port Access page opens.
2. Click the port name of the appropriate target server. The Port Action menu appears.
3. Choose Power On. A confirmation message appears.

► **To power off a target server:**

1. From the KSX II Remote Console, click the Port Access tab to open it. The Port Access page opens.
2. Click the port name of the appropriate target server. The Port Action menu appears.
3. Choose Power Off. A confirmation message appears.

Disconnecting KVM Target Servers

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

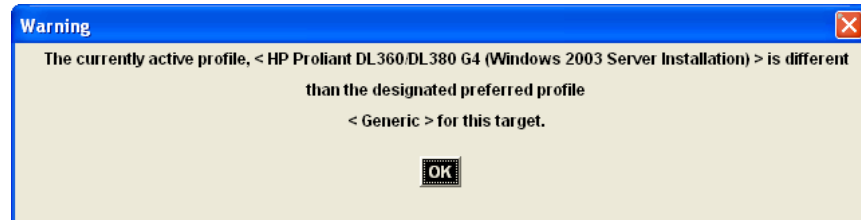
► **To disconnect a target server:**

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

Tip: You can also close the Virtual KVM Client window by selecting Connection > Exit from the Virtual KVM menu.

Choosing USB Profiles

When you connect to a KVM target server for the first time, as described in **Connecting to a KVM Target Server** (on page 47), the preferred USB profile for the port is automatically used. If you have connected to the target server previously using a different profile, the USB profile from the last connection is used. You are alerted to the use of a profile other than the preferred profile by a warning similar to the following:



After you have connected to a target server, you can change the USB profile as necessary. By default, the profiles that appear under the USB Profile menu in the VKC are those that you are most likely to use. These profiles have been preselected by the administrator for use with the connected target server, based on your operational requirements. However, all profiles are available to be selected via the Other Profiles option on the USB Profile menu.

► To choose a USB profile:

1. Connect to a KVM target server as described in **Connecting to a KVM Target Server** (on page 47).
2. In VKC, choose a USB profile from the USB Profile menu.

The name of the profile indicates the operating system or server with which it should be used. See **USB Profiles** (on page 92) for details on USB profiles.

Connection Properties


Dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints.

The devices optimize KVM output not only for LAN use, but also for WAN use.

These devices can also control color depth and limit video output, offering an optimal balance between video quality and system responsiveness for any bandwidth.

The parameters in the Properties dialog can be optimized to suit your needs for different operating environments. Connection properties are saved across subsequent connections to generation 2 devices once they are set and saved.

► **To set the connection properties:**

1. Choose Connection > Properties or click the Connection Properties button  in the toolbar. The Properties dialog appears.
2. Choose the Connection Speed from the drop-down list. The device can automatically detect available bandwidth and not limit bandwidth use. However, you can also adjust this usage according to bandwidth limitations.
 - Auto
 - 1G Ethernet
 - 100 Mb Ethernet
 - 10 Mb Ethernet
 - 1.5 Mb (MAX DSL/T1)
 - 1 Mb (Fast DSL/T1)
 - 512 Kb (Medium DSL/T1)
 - 384 Kb (Slow DSL/T1)
 - 256 Kb (Cable)
 - 128 Kb (Dual ISDN)
 - 56 kb (ISP Modem)
 - 33 kb (Fast Modem)
 - 24 kb (Slow Modem)

Note that these settings are an optimization for specific conditions rather than an exact speed. The client and server always attempt to deliver video as quickly as possible on the network regardless of the current network speed and encoding setting. But the system will be most responsive when the settings match the real world environment.

3. Choose the Color Depth from the drop-down list. The device can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths.
 - 15-bit RGB Color
 - 8-bit RGB Color
 - 4-bit Color
 - 4-bit Gray
 - 3-bit Gray
 - 2-bit Gray
 - Black and White

Important: For most administrative tasks (server monitoring, reconfiguring, and so on), the full 24-bit or 32-bit color spectrum made available by most modern video graphics cards is not necessary. Attempting to transmit such high color depths wastes network bandwidth.

4. Use the slider to select the desired level of Smoothing (15-bit color mode only). The level of smoothing determines how aggressively to blend screen regions with small color variation into a single smooth color. Smoothing improves the appearance of target video by reducing displayed video noise.
5. Click OK to set these properties.

Connection Information

► To obtain information about your Virtual KVM Client connection:

- Choose Connection > Info... The Connection Info window opens.

The following information is displayed about the current connection:

- Device Name - The name of the device.
- IP Address - The IP address of the device.
- Port - The KVM communication TCP/IP port used to access the target device.
- Data In/Second - Data rate in.
- Data Out/Second - Data rate out.
- Connect Time - The duration of the connect time.
- FPS - The frames per second transmitted for video.
- 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 copy this information:


- Click Copy to Clipboard. The information is available to be pasted into the program of your choice.

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 the computer on which the Virtual KVM Client (VKC) is running (your client PC).

Macros are stored on the client PC and are PC-specific. Therefore, 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.

Keyboard macros created in Virtual KVM Client (VKC) cannot be used in Active KVM Client (AKC) or vice versa.

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.

Import Macros

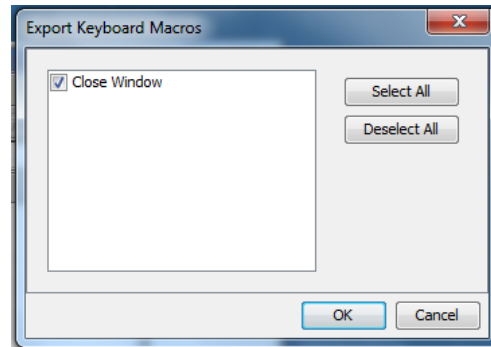
► To import macros:

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, do the following:**

- 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: The Calibrate Color command applies to the current connection only.

► **To calibrate the color, do the following:**

- Choose Video > Calibrate Color, or click the Calibrate Color button

 in the toolbar.

The target device screen updates its color calibration.

Adjusting 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.

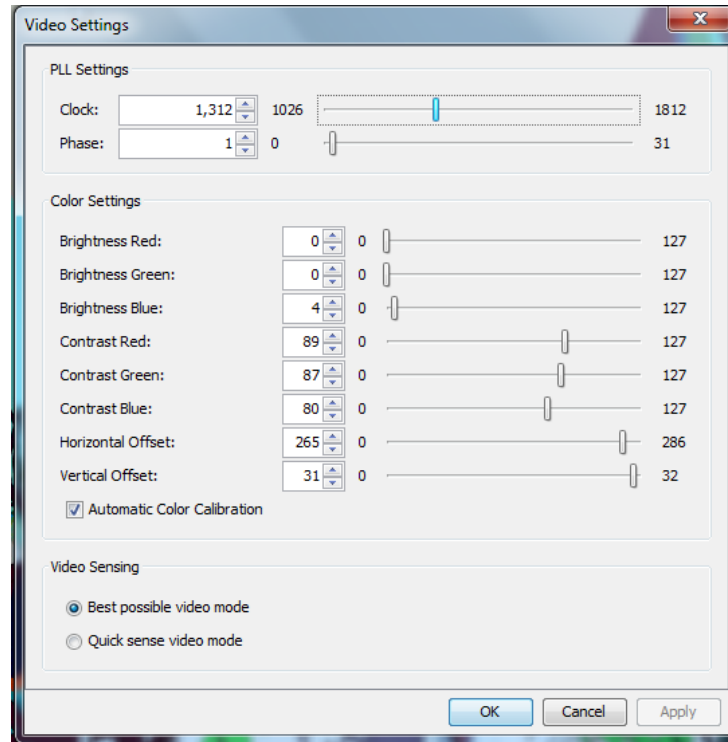
- i. Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor.
 - j. Vertical Offset - Controls the vertical positioning of the target server display on your monitor.
3. Select Automatic Color Calibration to enable this feature.
 4. Select the video sensing mode:
 - 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)

You are able to 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.

Changing the Maximum Refresh Rate

If the video card you are using on the target uses custom software, and you are accessing the target through the Virtual KVM Client (VKC) or Multi-Platform Client (MPC), you may need to change the maximum refresh rate of the monitor in order for the refresh rate to take effect on the target.

► **To adjust the monitor refresh rate:**

1. In Windows®, select Display Properties > Settings > Advanced to open the Plug and Play dialog.
2. Click on the Monitor tab.
3. Set the 'Screen refresh rate'.
4. Click OK and then OK again to apply the setting.

Mouse Options

When in dual mouse mode, and provided the option is properly configured, the mouse cursors align.

In dual mouse mode, when controlling a target server, the Remote Console displays two mouse cursors: one belonging to your KSX II client workstation, and the other belonging to the target server.

You can operate in either single mouse mode or dual mouse mode.

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.

Note that the black connector on the DVUSB CIMs are used for the keyboard and mouse. The gray connector is used for virtual media.

Keep both 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 using relative mouse positions. Standard Mouse mode requires that mouse acceleration is disabled and other mouse parameters are set correctly in order for the client and server mouse to stay synchronized.

► 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 pointer with KVM Client mouse pointer.

► **To synchronize the mouse, do one of the following:**

- Choose Mouse > Synchronize Mouse or click the Synchronize Mouse button  in the toolbar.


Note: This option is available only in Standard and Intelligent mouse modes.

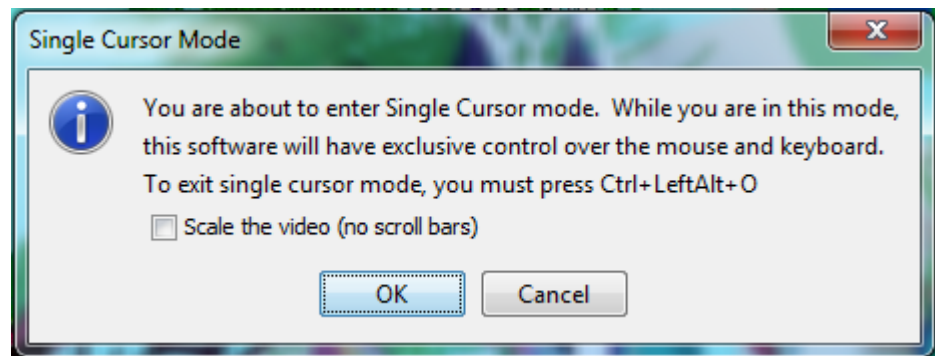
Single Mouse Mode

Single Mouse mode uses only the target server mouse cursor and the local mouse pointer no longer appears onscreen.

Note: Single mouse mode does not work on Windows or Linux targets when 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.

Smart Cards

Using the KSX II, 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 65).

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 249) 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 290)
- Supported Computer Interface Module (CIMs) Specifications
- **Supported and Unsupported Smart Card Readers** (on page 292)

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.

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.

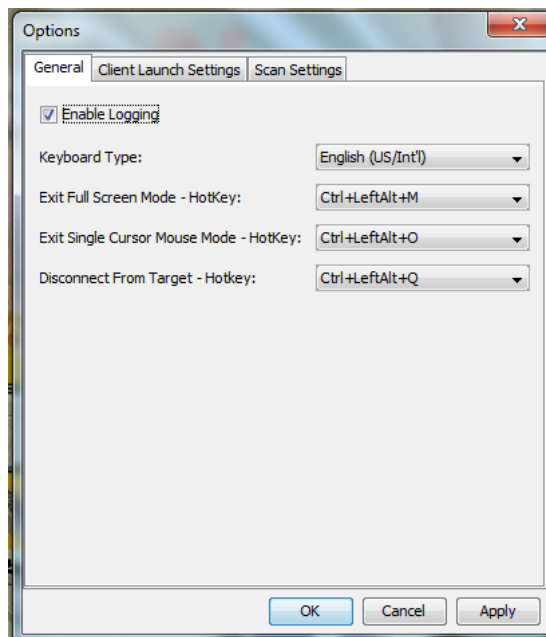
Enable this hotkey to allow users to quickly disconnect from the target.

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.

5. 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)
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.

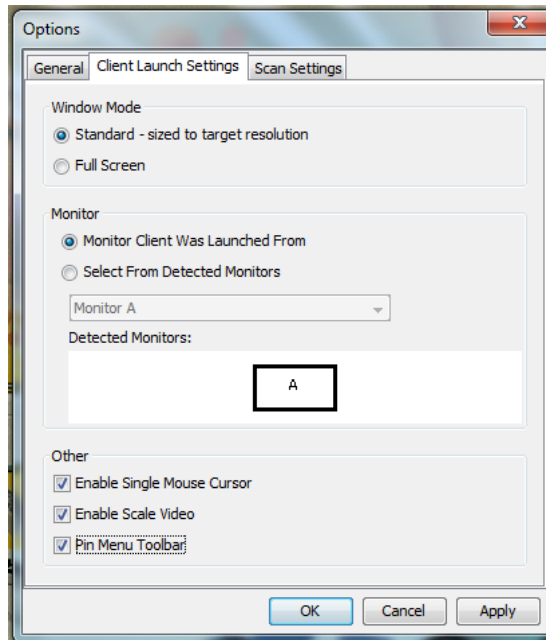
Client Launch Settings

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.

3. Click OK.



Configure Scan Settings in VKC and AKC

The KSX II provides 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 Virtual KVM Client (VKC) or Active KVM Client (AKC). See [Scanning Ports - Remote Console](#)

Use the Scan Settings tab to customize the scan interval and default display options.

► 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.

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 67).

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 67).

► 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.

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)

Please note this client is used by various Raritan products. As such, references to other products may appear in this section of 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 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 VKC
- Direct port access configuration (see Enabling Direct Port Access via URL)
- AKC server certification validation configuration (see **Prerequisites for Using AKC** (on page 75))
- AKC automatically loads favorites, VKC does not. See **Managing Favorites** (on page 39)

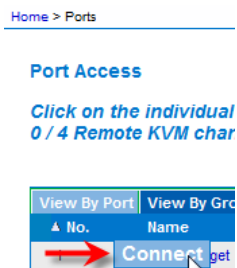
For details on using the features, see Virtual KVM Client (VKC) Help.

Connect to a Target Server

Once you have logged on to the KSX II Remote Console, access target servers via the Virtual KVM Client (VKC) 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 for details on additional available menu options.

AKC Supported Microsoft .NET Framework

The Active KVM Client (AKC) requires Windows .NET® version 3.5, 4.0 or 4.5. AKC works with both 3.5 and 4.0 installed.

AKC Supported Operating Systems

When launched from Internet Explorer®, the Active KVM Client (AKC) allows you to reach target servers via the KSX II.

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)

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 3.5 or 4.0 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® 8 (and later)

If you attempt to open AKC from a browser other than Internet Explorer 8 (and later), you will receive an error message instructing you to check your browser and to switch to Internet Explorer.

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 KSX II 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.

Multi-Platform Client (MPC)

Raritan Multi-Platform Client (MPC) is a graphical user interface for the Raritan product lines, providing remote access to target servers connected to Raritan KVM over IP devices. For details on using MPC, see the **KVM and Serial Access Clients Guide** available on Raritan's website on the same page as the user guide. Instructions on launching MPC are provided there.

Please note this client is used by various Raritan products. As such, references to other products may appear in this section of help.

Launching MPC from a Web Browser

Important: Regardless of the browser you use, you must allow pop-ups from the Dominion device's IP address in order to open MPC.

Important: Only Macs with an Intel® processor can run JRE 1.6 and, therefore, be used as a client. Mac 10.5.8 does not support MPC as a standalone client.

1. To open MPC from a client running any supported browser, type `http://IP-ADDRESS/mpc` into the address line, where IP-ADDRESS is the IP address of your Raritan device. MPC opens in a new window.

Note: The Alt+Tab command toggles between windows only on the local system.

When MPC opens, the Raritan devices that were automatically detected and which are found on your subnet are displayed in the Navigator in tree format.

2. If your device is not listed by name in the navigator, add it manually:
 - a. Choose Connection > New Profile. The Add Connection window opens.
 - b. In the Add Connection window, type a device Description, specify a Connection Type, add the device IP address, and click OK. These specifications can be edited later.
3. In the Navigator panel on the left of the page, double-click the icon that corresponds to your Raritan device to connect to it.

Note: Depending on your browser and browser security settings, you may see various security and certificate check and warning messages. It is necessary to accept the options in order to open MPC.

Note: If you are using Firefox 3.0.3, you may experience problems launching the application. If this occurs, clear the browser cache and launch the application again.

Launching MPC on Mac Lion Clients

If you are using Mac® Lion on your client, Raritan's Multi-Platform Client (MPC) does not launch. Use the following workaround to launch MPC.

Delete the JavaApplicationStub from the install, and create a link from the correct JavaApplicationStub.

- `rm /Applications/Raritan/Raritan Multi-Platform Client/<MPC Version>/Raritan Multi-Platform Client.app/Contents/MacOS/JavaApplicationStub`
- `ln -s /System/Library/Frameworks/JavaVM.framework/Resources/MacOS/JavaApplicationStub /Applications/Raritan/Raritan Multi-Platform Client/<MPC Version>/Raritan Multi-Platform Client.app/Contents/MacOS/JavaApplicationStub`

To run, use:

- `/Applications/Raritan/Raritan Multi-Platform Client/<MPC Version>/Raritan Multi-Platform Client.app/Contents/MacOS/JavaApplicationStub`

Raritan Serial Console (RSC)

Opening RSC from the Remote Console

- To open the Raritan Serial Console (RSC) from the Remote Console:

1. Select the Port Access tab.

Port Access

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

Port Number	Port Name	Port Type	Status	Available
1	Vlin Target	VM	up	idle
2	Dominion_KSX2_Port2	Not Available	down	idle
3	Dominion_KSX2_Port3	Not Available	down	idle
4	KSX-Q2 Admin	VM	up	idle
5	Dominion_KSX2_Port5	Not Available	down	idle
6	Dominion_KSX2_Port6	Not Available	down	idle
7	Dominion_KSX2_Port7	Not Available	down	idle
8	Dominion_KSX2_Port8	Not Available	down	idle
9	Cisco 2501	Serial	up	idle
10	SP-2	Serial	up	idle
11	Serial Port 3	Serial	up	idle
12	Serial Port 4	Serial	up	idle
13	SP - 5	Serial	up	idle
14	Serial Port 6	Serial	up	idle
15	Serial Port 7	Serial	up	idle
16	Serial Port 8	Serial	up	idle

2. Click the name of the serial port you want to access for the RSC.

Note: A security pop-up screen appears only if you used https to connect to the RSC.

3. If you're using Dominion DSX:

- Click Yes. A Warning - Security pop-up screen appears.
- Click Yes to access the Raritan Serial Console from the Port page.

Note: If you click Always, you will not receive the security page for future access.

- The Raritan Serial Console window appears.

If you're using Dominion KSX or KX:

- Click Connect to start connecting to the target port for RSC, and the Raritan Serial Console window appears.
- The Raritan Serial Console window appears.

Note: Download the standalone Raritan Serial Console from the Raritan website (www.raritan.com) on the Support page.

► **To open RSC from the Windows® desktop:**

1. Double-click the shortcut or use the Start menu to open the standalone RSC. The Raritan Serial Console Login connection properties window appears.
2. Enter the device's IP address, account information, and the desired target (port).
3. Click Start. RSC opens with a connection to the port.

Note: If you experience unrecognized characters or blurry pages in the RSC window due to localization support, try changing the font to Courier New. Click Emulator > Settings > Display and select Courier New for Terminal Font Properties or GUI Font Properties.

Note: When RSC connects to a serial target, hitting Ctrl + _ or Ctrl + ^ + _ does not cause information to be sent. However, hitting the Ctrl + Shift + _ or the Ctrl + Shift + ^ will cause information to be sent.

► **To open RSC on Sun™ Solaris™:**

1. Open a terminal window and change to the directory where you installed the RSC.
2. Type `./start.sh` and press Enter to open RSC.
3. Double-click the desired device to establish a connection.
4. Type your user name and password.
5. Click OK to log on.

Chapter 4 Rack PDU (Power Strip) Outlet Control

In This Chapter

Overview	80
Turning Outlets On/Off and Cycling Power	81

Overview

The KSX II allows you to control Raritan PX and RPC series rack PDU (power strip) outlets. Once a PX or RPC series is setup and then attached to the KSX II, the rack PDU and its outlets can be controlled from the Powerstrip page in the KSX II interface. This page is accessed by clicking on the Power menu at the top of the page.

The Powerstrip page will display rack PDUs attached to the KSX II for which the user has been granted appropriate port access permissions.

*Note: For information on setting up a PX, see the **Raritan PX User Guide**.*

From the Powerstrip page, you are able to turn the outlets on and off, as well as cycle their power. You are also able to view the following power strip and outlet information:

- Powerstrip Device Information:
 - 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 ports associated with the outlet.

Initially, when you open the Powerstrip page, the power strips that are currently connected to the KSX II are displayed in the Powerstrip drop-down. Additionally, information relating to the currently selected power strip is displayed. If no power strips are connected to the KSX II, a message stating "No powerstrips found" will be displayed in the Powerstrip Device section of the page.

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	

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.

Chapter 5 Virtual Media

All KSX II 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 KSX II 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, or RC4 encryption.

In This Chapter

Prerequisites for Using Virtual Media	83
Mounting Local Drives	84
Supported Tasks Via Virtual Media	85
Supported Virtual Media Types	85
Supported Virtual Media Operating Systems	86
Number of Supported Virtual Media Drives	86
Connecting and Disconnecting from Virtual Media	87
Virtual Media in a Windows XP Environment	89
Virtual Media in a Linux Environment	89
Virtual Media in a Mac Environment	90
Virtual Media File Server Setup (File Server ISO Images Only)	91

Prerequisites for Using Virtual Media

KSX II Virtual Media Prerequisites

- For users requiring access to virtual media, the KSX II 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** (on page 193) 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

Note that the black connector on the DVUSB CIMs are used for the keyboard and mouse. The gray connector is used for virtual media.

Keep both 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

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)
- Digital audio devices*

Note: ISO9660 is the standard supported by Raritan. However, other ISO standards can be used.

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.

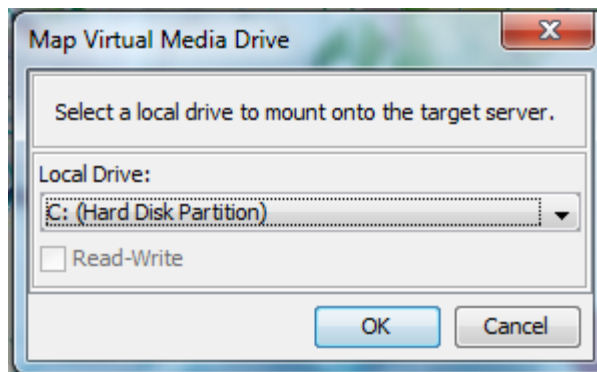
This need not be the first step, but it must be done prior to attempting to access this media.

Connecting and Disconnecting from Virtual Media

Access a Virtual Media Drive on a Client Computer

► **To access a virtual media drive on the client computer:**

1. From the Virtual 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 85) 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 Virtual 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 a making a virtual media connection.

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.

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 umount /dev/disk1s1` to unmount the device and `diskutil mount /dev/disk1s1` to remount it.

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 88).

► **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 6 USB Profiles

In This Chapter

Overview	92
CIM Compatibility	93
Available USB Profiles.....	93
Selecting Profiles for a KVM Port	99

Overview

To broaden the KSX II'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 KSX II 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** (see "**Virtual KVM Client (VKC)**" on page 46), 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.

A CIM that has not had its firmware upgraded supports a broad range of configurations (keyboard, mouse, CD-ROM, and removable drive), but will not be able to make use of profiles optimized for particular target configurations. Given this, existing CIMs should be upgraded with latest firmware in order to access USB profiles.

Until existing CIMs are upgraded, they will be able to provide functionality equivalent to the 'Generic' USB profile.

CIM firmware is automatically upgraded during a firmware upgrade, but CIMs that have not had their firmware upgraded can be upgraded as described in Upgrading CIMs.

Available USB Profiles

The current release of the KSX II 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	<p>Dell PowerEdge 1950/2950/2970/6950/R200 BIOS</p> <p>Use either this profile or 'Generic' profile for Dell PowerEdge 1950/2950/2970/6950/R200 BIOS.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ None
BIOS Dell OptiPlex™ Keyboard and Mouse Only	<p>Dell OptiPlex BIOS Access (Keyboard and Mouse Only)</p> <p>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.</p> <p>Notice:</p> <ul style="list-style-type: none"> ▪ Optiplex 210L/280/745/GX620 requires D2CIM-DVUSB with 'Generic' profile to support virtual media <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ No virtual media support
BIOS Dell Optiplex 790	<p>Use this profile for Dell Optiplex 790 during BIOS operations.</p> <p>Warning:</p>

USB profile	Description
	<ul style="list-style-type: none"> ▪ USB enumeration will trigger whenever Virtual Media is connected or disconnected <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ 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	<p>Use this profile for Dell Optiplex 790 when using Keyboard Macros during BIOS operations. Only keyboard is enabled with this profile.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ Mouse is disabled. ▪ Virtual CD-ROM and disk drives are disabled.
BIOS DellPowerEdge Keyboard and Mouse Only	<p>Dell PowerEdge BIOS Access (Keyboard and Mouse Only)</p> <p>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.</p> <p>Notice:</p> <ul style="list-style-type: none"> ▪ 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 <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ Absolute mouse synchronization™ not supported ▪ No virtual media support
BIOS ASUS P4C800 Motherboard	<p>Use this profile to access BIOS and boot from Virtual Media on Asus P4C800-based systems.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ Virtual CD-ROM and disk drives cannot be used simultaneously

USB profile	Description
BIOS Generic	<p>BIOS Generic</p> <p>Use this profile when Generic OS profile does not work on the BIOS.</p> <p>WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ 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	<p>HP ProLiant DL145 PhoenixBIOS</p> <p>Use this profile for HP ProLiant DL145 PhoenixBIOS during OS installation.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ USB bus speed limited to full-speed (12 MBit/s)
BIOS HP Compaq® DC7100/DC7600	<p>BIOS HP Compaq DC7100/DC7600</p> <p>Use this profile to boot the HP Compaq DC7100/DC7600 series desktops from virtual media.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS IBM ThinkCentre Lenovo	<p>IBM Thinkcentre Lenovo BIOS</p> <p>Use this profile for the IBM® Thinkcentre Lenovo system board (model 828841U) during BIOS operations.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ 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	<p>Use this profile to enable virtual media functionality when D2CIM-VUSB or D2CIM-DVUSB is connected to the Advanced Management Module.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ Virtual CD-ROM and disk drives cannot be used simultaneously

USB profile	Description
BIOS Lenovo ThinkPad T61 & X61	<p>BIOS Lenovo ThinkPad T61 and X61 (boot from virtual media)</p> <p>Use this profile to boot the T61 and X61 series laptops from virtual media.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ USB bus speed limited to full-speed (12 MBit/s)
Generic	<p>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.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ None
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	<p>HP Proliant DL360/DL380 G4 (HP SmartStart CD)</p> <p>Use this profile for the HP Proliant DL360/DL380 G4 series server when installing OS using HP SmartStart CD.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ USB bus speed limited to full-speed (12 MBit/s) ▪ Absolute mouse synchronization™ not supported
HP Proliant DL360/DL380 G4 (Windows 2003® Server Installation)	<p>HP Proliant DL360/DL380 G4 (Windows 2003 Server Installation)</p> <p>Use this profile for the HP Proliant DL360/DL380 G4 series server when installing Windows 2003 Server without the help of HP SmartStart CD.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ USB bus speed limited to full-speed (12 MBit/s)
Linux®	<p>Generic Linux profile</p> <p>This is the generic Linux profile; use it for Redhat Enterprise Linux, SuSE Linux Enterprise Desktop and similar distributions.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ Absolute mouse synchronization™ not supported
BIOS Mac®	<p>BIOS Mac</p> <p>Use this profile for Mac BIOS.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> ▪ Absolute mouse synchronization™ is not supported ▪ Virtual CD-ROM and disk drives cannot be used simultaneously <p>If you use this USB profile, see Mouse Modes when Using the Mac Boot Menu (on page 99) for information mouse modes</p>

USB profile	Description
	when using the Mac Boot Menu
MAC OS X® 10.4.9 (and later)	<p>Mac OS X version 10.4.9 (and later)</p> <p>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.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> Virtual CD-ROM and disk drives cannot be used simultaneously
RUBY Industrial Mainboard (AwardBIOS)	<p>RUBY Industrial Mainboard (AwardBIOS)</p> <p>Use this profile for the RUBY-9715VG2A series industrial mainboards with Phoenix/AwardBIOS v6.00PG.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> USB bus speed limited to full-speed (12 MBit/s) Virtual CD-ROM and disk drives cannot be used simultaneously
Supermicro Mainboard Phoenix (AwardBIOS)	<p>Supermicro Mainboard Phoenix AwardBIOS</p> <p>Use this profile for the Supermicro series mainboards with Phoenix AwardBIOS.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> Virtual CD-ROM and disk drives cannot be used simultaneously
Suse 9.2	<p>SuSE Linux 9.2</p> <p>Use this for SuSE Linux 9.2 distribution.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> Absolute mouse synchronization™ not supported USB bus speed limited to full-speed (12 MBit/s)
Troubleshooting 1	<p>Troubleshooting Profile 1</p> <ul style="list-style-type: none"> 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 <p>WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected.</p>
Troubleshooting 2	Troubleshooting Profile 2

USB profile	Description
	<ul style="list-style-type: none"> 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 <p>WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected.</p>
Troubleshooting 3	<p>Troubleshooting Profile 3</p> <ul style="list-style-type: none"> 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 <p>WARNING: USB enumeration will trigger whenever virtual media is connected or disconnected.</p>
Use Full Speed for Virtual Media CIM	<p>Use Full Speed for virtual media CIM</p> <p>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.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> USB bus speed limited to full-speed (12 MBit/s)
Use Full Speed for Keyboard and Mouse USB	<p>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.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> 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 USB profiles in, 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 KSX II 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 KSX II Remote or Local Console.

It is the administrator that designates the profiles that are most likely to be needed for a specific target. These profiles are then available for selection via Multi-Platform Client (MPC), Active KVM Client (AKC) and 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 Multi-Platform Client (MPC), Active KVM Client (AKC) and Virtual KVM Client (VKC)..

For information about assigning USB profiles to a KVM port, see **Configuring USB Profiles (Port Page)** (on page 158).

Chapter 7 User Management

In This Chapter

User Groups	100
Users	107
Authentication Settings	111
Changing a Password	123

User Groups

The KSX II stores an internal list of all user and group names to determine access authorization and permissions. This information is stored internally in an encrypted format. There are several forms of authentication and this one is known as local authentication. All users have to be authenticated. If the KSX II is configured for LDAP/LDAPS or RADIUS, that authentication is processed first, followed by local authentication.

Every KSX II 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 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 KSX II.

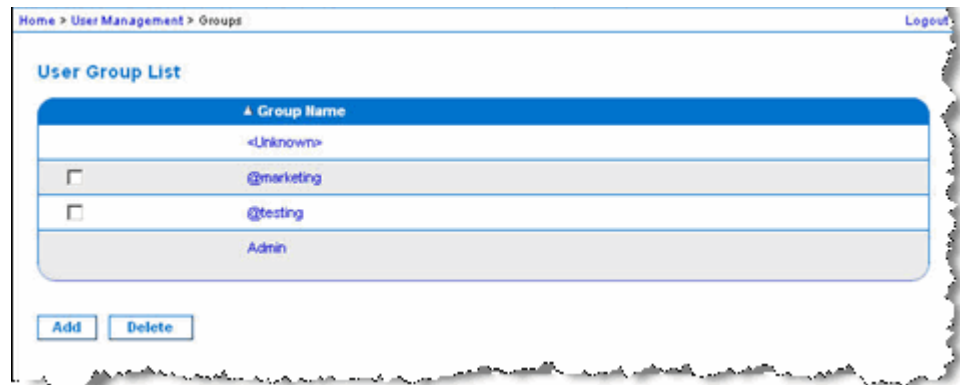
User Group List

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 KSX II 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 device uses group information to determine the user's permissions, such as which server ports are accessible, whether rebooting the device is allowed, and other features.

Adding a New User Group

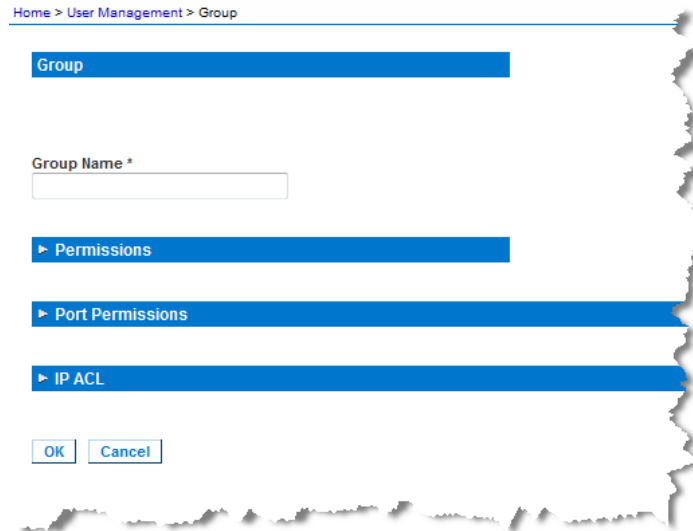
► To add a new user group:

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](#). See **Permissions** (on page 103).
4. Specify the server ports and the type of access for each user belonging to this group. See [Setting Port Permissions](#). See **Port Permissions** (on page 104).
5. Set the IP ACL. This feature limits access to the KSX II 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 \(Access Control List\)](#). See **Group-Based IP ACL (Access Control List)** (on page 104).
6. Click OK.

Note: Several administrative functions are available within and from the KSX II Local Console. These functions are available only to members of the default Admin group.

Note: Both IPv4 and IPv6 addresses are supported.



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.

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	<p>Allows users and user groups with this permission to directly access the KSX II using an IP address when Local Access is enabled for the device in CC-SG. The device can be accessed from the Local Console, Remote Console, MPC, VKC, and AKC.</p> <p>When a device is accessed directly while it is under CC-SG management, access and connection activity is logged on the KSX II. User authentication is performed based on KSX II authentication settings.</p> <p><i>Note: The Admin user group has this permission by default.</i></p>
Device Settings	Network settings, date/time settings, port configuration (channel names, power associations), event management (SNMP, Syslog), virtual media file server setup
Diagnostics	Network interface status, network statistics, ping host, trace route to host, KSX II diagnostics
Maintenance	Backup and restore database, firmware upgrade, factory reset, reboot
Modem Access	Permission to use the modem to connect to the KSX II device
PC-Share	Simultaneous access to the same target by multiple users
Security	SSL certificate, security settings (VM Share, PC-Share), IP ACL
User Management	User and group management, remote authentication (LDAP/LDAPS/RADIUS), login settings

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.

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.

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 KSX II if your IP address is within a range that has been denied access.

This feature limits access to the KSX II device by users in the selected group to specific IP addresses. This feature 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, is processed first, and takes priority.

Important: The IP address 127.0.0.1 is used by the KSX II 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.

Rule #	Starting IP	Ending IP	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	ACCEPT <input type="button" value="v"/>

► **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 KSX II device.
 - Drop - IP addresses set to Drop are denied access to the KSX II 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.
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.
4. Set the IP ACL (optional). This feature limits access to the KSX II device by specifying IP addresses. See Group-Based IP ACL (Access Control List).
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 KSX II. This information is used to authenticate users attempting to access your KSX II.

Adding a New User

It is a good idea to define user groups before creating KSX II users because, when you add a user, you must assign that user to an existing user group. Refer to **Adding a New User Group** (on page 101) for more information.

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

*Note: A user name can be deactivated when the number of failed login attempts has exceeded the maximum login attempts set in the Security Settings page. Refer to **Security Settings** (on page 193) for more information.*

► **To add a new user:**

1. Open the User page by choosing User Management > Add New User or clicking the Add button 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. If there is a dialback number, type it in the Dialback Number field. Dialback numbers cannot contain any of the following characters or the log on will fail when it is attempted:

- " double quote
 - ' single quote
 - ; semicolon
 - \$ dollar sign
 - & and sign
 - ½ pipe symbol
6. Choose the group from the User Group drop-down list. The list contains all groups you have created in addition to the system-supplied default groups (<Unknown> (default setting), Admin, Individual Group).

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, refer to **Setting Permissions for an Individual Group** (on page 102).
 7. To activate the new user, select the Active checkbox. The default is activated (enabled).
 8. Click OK.

View KSX II User 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.

To view the ports each user is connected to, see **View Users by Port** (on page 109).

► **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 KSX II
- 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 the KSX II.

*Note: Logging users off disconnects the user from the target port and logs them off of the KSX II. See **Logging Users Off the KSX II (Force Logoff)** (on page 110) for information on forcibly logging users off.*

► To disconnect users from port:

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 KSX II (Force Logoff)

If you are an administrator, you are able to log off any authenticated user who is logged on to the KSX II. Users can also be disconnected at the port level. See ***Disconnecting Users from Ports*** (on page 109).

► To log a user off the KSX II:

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 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 KSX II is configured for remote authentication, the external authentication server is used primarily for the purposes of authentication, not authorization.

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

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** (see "**Implementing LDAP/LDAPS Remote Authentication**" on page 112) 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** (on page 116) 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 (through 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.
7. 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.
8. 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.

9. 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.
10. 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

11. In the Dialback Query String field, type the dialback query string.

Optional

If you are using Microsoft Active Directory, you must enter the following string: `msRADIUSCallbackNumber`. If you are not using Microsoft Active Directory, use the attribute string defined for that LDAP server.

Note: This string is case sensitive.

12. 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).

The screenshot shows a 'Server Configuration' dialog box with the following fields and options:

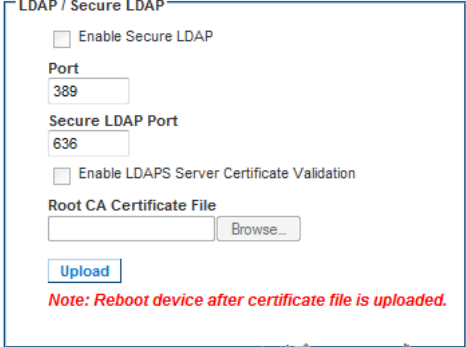
- Primary LDAP Server: [Text Input Field]
- Secondary LDAP Server (optional): [Text Input Field]
- Type of External LDAP Server: [Dropdown Menu] (Currently set to 'Generic LDAP Server')
- Active Directory Domain: [Text Input Field]
- User Search DN: [Text Input Field]
- DN of Administrative User (optional): [Text Input Field]
- Secret Phrase of Administrative User: [Text Input Field]
- Confirm Secret Phrase: [Text Input Field]
- Dialback Query String: [Text Input Field]

LDAP/Secure LDAP

13. Select the Enable Secure LDAP checkbox if you would like to use SSL. This will enable the Enable LDAPS Server Certificate Validation checkbox. Secure Sockets Layer (SSL) is a cryptographic protocol that allows KSX II to communicate securely with the LDAP/LDAPS server.
14. The default Port is 389. Either use the standard LDAP TCP port or specify another port.
15. The default Secure LDAP Port is 636. Either use the default port or specify another port. This field is only used when the Enable Secure LDAP checkbox is selected.
16. 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.

17. If needed, upload the Root CA Certificate File. This field is enabled when the Enable Secure LDAP option is selected. 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 KSX II in order for the new certificate to take effect.



LDAP / Secure LDAP

☐ Enable Secure LDAP

Port
389

Secure LDAP Port
636

☐ Enable LDAPS Server Certificate Validation

Root CA Certificate File
 Browse...

Upload

Note: Reboot device after certificate file is uploaded.

Test LDAP Server Access

18. The KSX II provides you with the ability to test the LDAP configuration from the Authentication Settings page due to the complexity sometimes encountered with successfully configuring the LDAP server and KSX II for remote authentication. To test the LDAP configuration, enter the login name and password in the "Login for testing" field and the "Password for testing" field respectively. This is the username and password you entered to access the KSX II and that the LDAP server will use to authenticate you. Click Test.
19. Once the test is completed, a message will be displayed that lets you know the test was successful or, if the test failed, a detailed error message will be displayed. It will display successful result or detail error message in failure case. It also can display group information retrieved from remote LDAP server for the test user in case of success.



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 fields is a button labeled "Test". The dialog box has a blue border and a shadow effect.

Returning User Group Information from Active Directory Server

The KSX II supports user authentication to Active Directory® (AD) without requiring that users be defined locally on the KSX II. 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 KSX II 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 KSX II 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 KSX II:

1. Using the KSX II, 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 KSX II users to the groups created in step 2.

4. From the KSX II, enable and configure your AD server properly. See Implementing LDAP/LDAPS Remote Authentication.


Important Notes

- Group Name is case sensitive.
- The KSX II 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 KSX II group configuration, the KSX II 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 KSX II 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 KSX II 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 KSX II 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.

Home > User Management > Authentication Settings

Authentication Settings

☐ Local Authentication

☐ LDAP

☒ RADIUS

> LDAP

▼ RADIUS

Primary RADIUS Server

Shared Secret

Authentication Port

1812

Accounting Port

1813

Timeout (in seconds)

1

Retries

3

Secondary RADIUS Server

Shared Secret

Authentication Port

1812

Accounting Port

1813

Timeout (in seconds)

1

Retries

3

Global Authentication Type

PAP ▼

OK

Reset To Defaults

Cancel

Cisco ACS 5.x for RADIUS Authentication

If you are using a Cisco ACS 5.x server, after you have configured the KSX II 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 KSX II 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 KSX II 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 KSX II modem will use to dial back to the user account.

RADIUS Communication Exchange Specifications

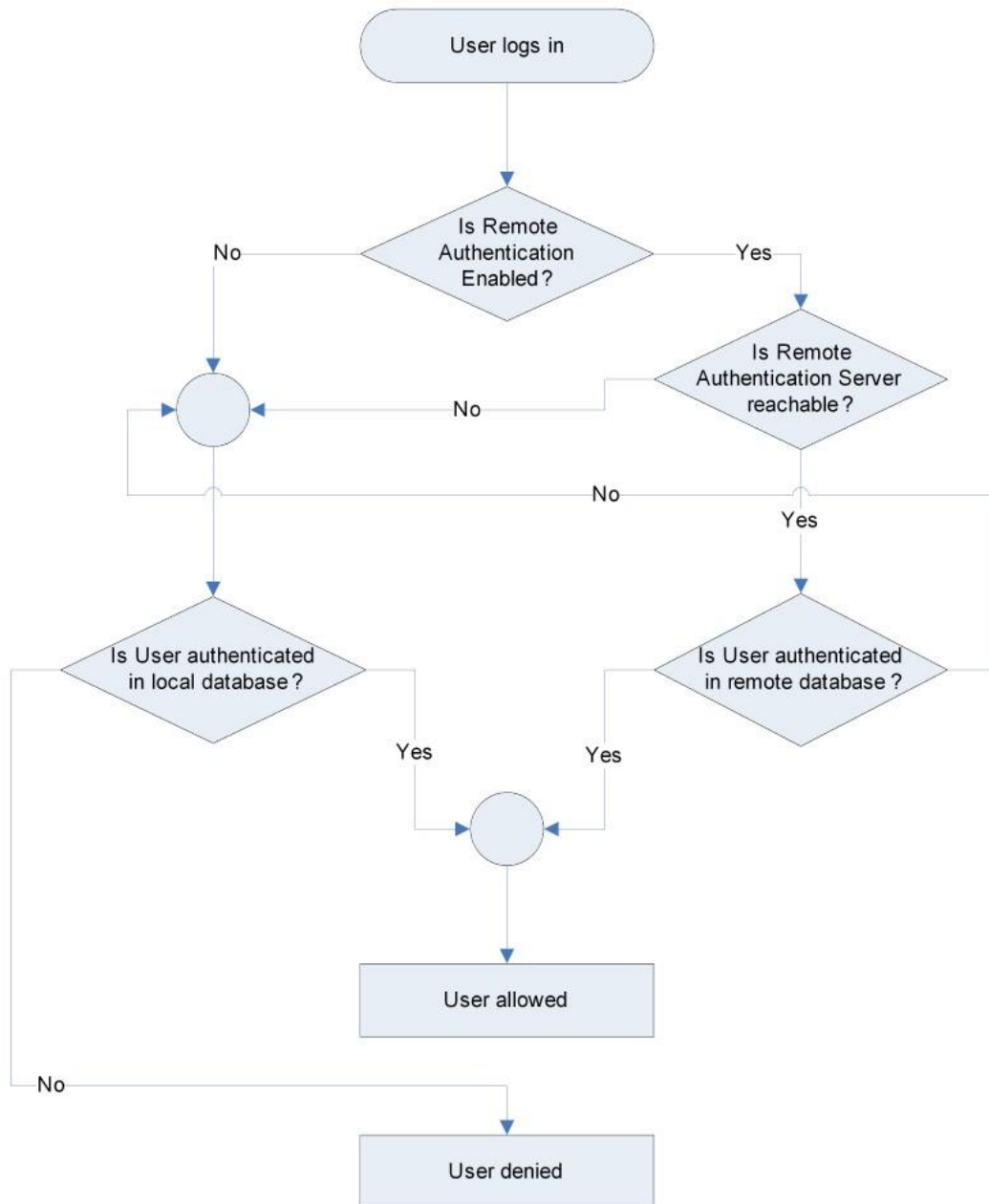
The KSX II sends the following RADIUS attributes to your RADIUS server:

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 KSX II.
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 KSX II.
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 KSX II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

User Authentication Process

Remote authentication follows the process specified in the flowchart below:



Changing a Password

► **To change your KSX II 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 196) in online help.*

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

Chapter 8 Device Management

In This Chapter

Network Settings	124
Configuring Ports	128
Device Services	163
Configuring Modem Settings	173
Configuring Date/Time Settings	174
Event Management	175
Connect and Disconnect Scripts	183
Port Keywords	189
Port Group Management	191
Changing the Default GUI Language Setting	192

Network Settings

Use the Network Settings page to customize the network configuration (for example, the IP address, discovery port, and LAN interface parameters) for your KSX II.

There are two options available to set up your IP configuration:

- None (default) - This is the recommended option (static IP). Since the KSX II is part of your network infrastructure, you most likely do not want its IP address to change frequently. This option allows you to set the network parameters.
- DHCP - With this option, the IP address is automatically assigned by a DHCP server.

► **To change the network configuration:**

1. Choose Device Settings > Network. The Network Settings page opens.
2. Update the Network Basic Settings. See Network Basic Settings.
3. Update the LAN Interface Settings. See **LAN Interface Settings** (on page 127).
4. Click OK to set these configurations. If your changes require rebooting the device, a reboot message appears.

► **To reset to factory defaults:**

- Click Reset to Defaults.

Network Basic Settings

These procedures describe how to assign an IP address on the Network Settings page. For complete information about all of the fields and the operation of this page, see **Network Settings** (on page 124).

Assign the KSX II an IP Address

► **To assign an IP address to the KSX II:**

1. Choose Device Settings > Network. The Network Settings page opens.
2. Specify a meaningful Device Name for your KSX II device.
Up to 32 alphanumeric and valid special characters, no spaces between characters.
3. Next, configure the IPv4, IPv6 and DNS settings.

Configure the IPv4 Settings

1. In the IPv4 section, enter or select the appropriate IPv4-specific network settings:
 - a. Enter the IP Address if needed. The default IP address is 192.168.0.192.
 - b. Enter the Subnet Mask. The default subnet mask is 255.255.255.0.
 - c. Enter the Default Gateway if None is selected from the IP Auto Configuration drop-down.
 - d. Enter the Preferred DHCP Host Name if DHCP is selected from the IP Auto Configuration drop-down.
 - e. Select the IP Auto Configuration. The following options are available:
 - None (Static IP) - This option requires you manually specify the network parameters.

This is the recommended option because the KSX II is an infrastructure device, and its IP address should not change.

Select this option if you want to ensure redundant failover capabilities should the primary Ethernet port (or the switch/router to which it is connected) fail. If it fails, KSX II fails over to the secondary network port with the same IP address, ensuring there is not interruption.
 - DHCP - Dynamic Host Configuration Protocol is used by networked computers (clients) to obtain unique IP addresses and other parameters from a DHCP server.

With this option, network parameters are assigned by the DHCP server.

If DHCP is used, enter the Preferred host name (DHCP only). Up to 63 characters.

2. Next, configure IPv6 and/or DNS settings.

Configure the IPv6 Settings

1. If using IPv6, enter or select the appropriate IPv6-specific network settings in the IPv6 section:
 - a. Select the IPv6 checkbox to activate the fields in the section and enable IPv6 on the device.
 - b. Enter a Global/Unique IP Address. This is the IP address assigned to the KSX II.
 - c. Enter the Prefix Length. This is the number of bits used in the IPv6 address.
 - d. Enter the Gateway IP Address.
 - e. Link-Local IP Address. This address is automatically assigned to the device, and is used for neighbor discovery or when no routers are present. **Read-Only**
 - f. Zone ID. Identifies the device the address is associated with. **Read-Only**
 - g. Select an IP Auto Configuration option:
 - None (Static IP) - this option requires you manually specify the network parameters.

This is the recommended option because the KSX II is an infrastructure device, and its IP address should not change.

Select this option if you want to ensure redundant failover capabilities should the primary Ethernet port (or the switch/router to which it is connected) fail. If it fails, KSX II switches to the secondary network port with the same IP address, ensuring there is no interruption.

If None is selected, the following Network Basic Settings fields are enabled: Global/Unique IP Address, Prefix Length, and Gateway IP Address allowing you to manually set the IP configuration.
 - Router Discovery - use this option to automatically assign IPv6 addresses that have Global or Unique Local significance beyond that of the Link Local, which only applies to a directly connected subnet.
2. Next, configure DNS settings.

Configure the DNS Settings

1. Select Obtain DNS Server Address Automatically if DHCP is selected and Obtain DNS Server Address is enabled. When Obtain DNS Server Address Automatically, the DNS information provided by the DHCP server will be used.
2. If Use the Following DNS Server Addresses is selected, whether or not DHCP is selected, the addresses entered in this section is used to connect to the DNS server.

Enter the following information if the Following DNS Server Addresses is selected. These addresses are the primary and secondary DNS addresses used if the primary DNS server connection is lost due to an outage.

- a. Primary DNS Server IP Address
 - b. Secondary DNS Server IP Address
3. When finished, click OK.

Your KSX II device is now network accessible.

LAN Interface Settings

The current parameter settings are identified in the Current LAN interface parameters field.

1. Choose Device Settings > Network. The Network Settings page opens.
2. Choose the LAN Interface Speed & Duplex from the following options:
 - Autodetect (default option)
 - 10 Mbps/Half - Both LEDs blink
 - 10 Mbps/Full - Both LEDs blink
 - 100 Mbps/Half - Yellow LED blinks
 - 100 Mbps/Full - Yellow LED blinks
 - 1000 Mbps/Full (gigabit) - Green 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 286) for more information.

3. Select the Enable Automatic Failover checkbox to allow the KSX II to automatically recover its network connection using a second network port if the active network port fails.

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

When this option is enabled, the following two fields are used:

- Ping Interval (seconds) - Ping interval determines how often the KSX II checks the status of the network path to the designated gateway. The default ping interval is 30 seconds.
- Timeout (seconds) - Timeout determines how long a designated gateway remains unreachable via the network connection before a fail over occurs.

Note: The ping interval and timeout can be configured to best meet the local network conditions. The timeout should be set to allow for at least two or more ping requests to be transmitted and responses returned. For example, if a high rate of failover is observed due to high network utilization, the timeout should be extended to 3 or 4 times the ping interval.

4. Select the Bandwidth.
5. Click OK to apply the LAN settings.

Configuring Ports

Access the Port Configuration Page

► **To access a port configuration:**

1. 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.

2. 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.
 - For rack PDUs, the Port page for rack PDUs (power strips) is opened. From this page, you can name the rack PDUs and their outlets.

Port Configuration Page

The Port Configuration page displays a list of the KSX II ports.

When a port's status is down, Not Available is displayed as its status. A port may be down when the port's CIM is removed or powered down.

Note: For blade chassis, the blade chassis name can be changed but its blade slot names cannot be changed.

Home > Device Settings > Port Configuration

Port Configuration

No.	Name	Type
1	HDMI Target	DVM-HDMI
2	Dominion-K02_Port2	DVM-DVI
3	Low Cost DVM (PQ20540016)	Dual-VM
4	Windows XP SP3	DCIM
5	DR-Dominion-K02_Port13	DVM-DP
6	Dominion-K02_Port19	DCIM
7	Dominion-K02_Port7	Dual-VM
8	pc-ix3-update	Not Available
9	KX832-60-234-Tier5	TierDevice
10	ix832-60-241-tier3	TierDevice
11	KX832-61-14-Tier1	TierDevice
12	Dominion_K03_Port12	Not Available
13	KX832-60-163-Tier2	TierDevice
14	DnsPort RHEL 5.5 secondary	Not Available

Port Number

Numbered from 1 to the total number of ports available for the KSX II device.

Port Name

Ports with no CIM connected or with a blank CIM name, a default port name of is assigned, where Port# is the number of the KSX II physical port.

Ports that are currently not connected to the KSX II via a CIM have a status of Not Available.

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

- Rename the port. When a CIM is attached the CIM name will be used.
- 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 CIMs
- 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 KVM Switches

The KSX II allows tier attachments to generic analog KVM switches supporting hot key switching. A variety of KVM hot key sequences are provided to choose from. Select one to match the hot key sequence supported on the analog KVM switch connected to via this port. That will allow targets on the tiered analog KVM switch to be accessible from a consolidated port list on the Port Access page.

Important: In order 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 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.
8. Activate the targets that the KVM switch hot key sequence will be applied to. Indicate the KVM switch ports have targets attached by selecting 'Active' for each of the ports.
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. 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 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 of 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 rename. The Port Page opens.
3. Deselect the Active checkbox next to the KVM switch target port or URL to change its active status.
4. Click OK.

Configuring CIM Ports

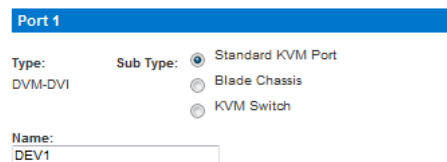
The KSX II supports the use of standard and virtual media CIMs to connect a server to the KSX II.

► **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.

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.



The screenshot shows a web interface for configuring a port. At the top, there is a blue header bar with the text "Port 1". Below this, the "Type" is set to "DVM-DVI". The "Sub Type" section has three radio button options: "Standard KVM Port" (which is selected), "Blade Chassis", and "KVM Switch". Below the "Sub Type" section, there is a "Name:" label followed by a text input field containing the text "DEV1".

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 720x400 Compensation if you are experiencing display issues when the target is using this resolution.
2. 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.

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.

Target Settings
<input type="checkbox"/> 720x400 Compensation
Display Native Resolution: 1600x1200@60 ▾

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 Selected Profiles to Other Ports			
Apply	Port Number	Port Name	Selected USB Profiles
<input checked="" type="checkbox"/>	1	Dominion - Win7	Generic
<input type="checkbox"/>	2	Dominion_Port2	Generic
<input type="checkbox"/>	3	Dominion - Win7	Generic
<input type="checkbox"/>	4	- Win7	Generic
<input type="checkbox"/>	7	HP Compaq - Win7	Generic

Apply a Native Display Resolution to Other CIMs

1. Apply the native display resolution to CIM 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
<input checked="" type="checkbox"/>	1	Dominion - Win7	1600x1200@60

Power Control

Power control is configured on the Port page. The Port page opens when you select a port that is connected to a target server from the Port Configuration page.

From the Port page, you can make power associations and change the port name to something more descriptive.

A server can have up to four (4) power associates 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 page.

See E. Power Strip of this guide for information on the physical connections between the KSX II and Dominion PX.

Port 1

Type:

PCIM

Name:

KX-local

Power Association

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

Target Settings

☐ 720x400 Compensation
 ☐ Use international keyboard for scan code set 3

Assigning a Name to the PX

The Port page opens when you select a port on the Port Configuration page. The port appears on this page when connected to a Raritan remote rack PDU (power strip). The Type and the Name fields are prepopulated.

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

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).

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

► To name the rack PDU (and outlets):

1. Change the Name of the rack PDU to something you will remember.
2. Change the (Outlet) Name, if desired. (Outlet names default to Outlet #.)
3. Click OK.

Associating KVM and Serial Target Servers to Outlets (Port Page)

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

The KVM and serial Port pages are different from each other with the exception of the Name and Port Association sections. Since the Power Association sections are the same, the steps below apply to both KVM and serial target servers.

► To make power associations (associate rack PDU outlets to 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. Choose the rack PDU from the Power Strip Name drop-down list.
2. For that rack PDU, choose the outlet from the Outlet Name drop-down list.
3. Repeat steps 1 and 2 for all desired power associations.
4. Click OK. A confirmation message is displayed.

► **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. The rack PDU/outlet association is removed and a confirmation message is displayed.

Configuring Blade Chassis

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

The blade chassis must be configured as a blade chassis subtype.

If the blade chassis type is supported, it is automatically detected once they are connected. If the type is not supported, the blade must be configured manually.

When a blade server 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. See Port Access Page (Remote Console Display).

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 hierarchal order, blade-chassis subtypes must be configured for the blade server chassis.

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.

The following blade chassis are supported:

- IBM BladeCenter® Models E and H
- Dell PowerEdge® 1855, 1955 and M1000e

A Generic option allows you to configure a blade chassis that is not included in the above list. HP BladeSystem c3000 and c7000, and Cisco UCS blade servers are supported via individual connections from the Dominion device to each blade. The ports are 'grouped' together into a chassis representation using the Port Group Management feature.

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

Two modes of operation are provided for blade chassis: manual configuration and auto-discovery, depending on the blade chassis capabilities. If a blade chassis is configured for auto-discovery, the Dominion device 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 KSX II only supports auto-discovery for AMM[1] as the acting primary management module.

The use of hot key sequences to switch KVM access to a blade chassis is also supported. For blade chassis that allow users to select a hot key sequence, those options will be provided on the Port Configuration page. 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, so this hot key sequence is applied by default when IBM BladeCenter H is selected during the configuration. See your blade chassis documentation for hot key sequence information.

You are able to configure the connection to a blade chassis web browser interface if one is available. 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 can be managed from the Virtual KVM Client (VKC), the Active KVM Client (AKC), Raritan's , and CC-SG. Managing blade servers via VKC, AKC and MPC is the same as managing standard target servers. See **Working with Target Servers** and the **CC-SG Administrators Guide** for more information. Any changes made to the blade chassis configuration in will be propagated to these client applications.

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


Important: If you move a blade chassis from one Dominion device port to another Dominion device port, interfaces that were added to the blade chassis node in CC-SG will be lost in CC-SG. All other information will be retained.

Generic Blade Chassis Configuration

The Generic Blade Chassis' selection provides only a manual configuration mode of operation. See Supported Blade Chassis Models, Supported CIMs for Blade Chassis, and ***Required and Recommended Blade Chassis Configurations*** (on page 155) for important, additional information when configuring the blade chassis. See ***Dell Chassis Cable Lengths and Video Resolutions*** (on page 315) for information on cable lengths and video resolutions when using Dell® chassis with the KSX II.

► To configure a chassis:

1. Connect the blade chassis to the KSX II. See Step 3: Connect the Equipment for details.
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.
6. Configure the blade chassis as applicable.
 - a. 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.
 - b. Administrative Module Primary IP Address/Host Name - 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.
7. Change the blade chassis name if needed.
8. 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.

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.

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. **Required**
- c. Username - Enter the username used to access the interface. **Optional**
- d. Password - Enter the password used to access the interface. **Optional**

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. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See **Tips for Adding a Web Browser Interface** (on page 149) for tips on adding a web browser interface. **Optional**
10. USB profile information does not apply to a generic configuration.
 11. In the Target Settings section, select 720x400 Compensation if you are experiencing display issues when the target is using this resolution.
 12. 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.

13. 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.

14. Click OK to save the configuration.

Dell Blade Chassis Configuration

See Supported Blade Chassis Models, Supported CIMs for Blade Chassis, and **Required and Recommended Blade Chassis Configurations** (on page 155) for important, additional information when configuring the blade chassis. See **Dell Chassis Cable Lengths and Video Resolutions** (on page 315) for information on cable lengths and video resolutions when using Dell® chassis with the KSX II.

► To add a blade chassis:

1. Connect the blade chassis to the KSX II. See Step 3: Connect the Equipment for details.
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). 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 KSX II 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 KSX II assigns the chassis a name. The default naming convention for the blade chassis by the KSX II 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.

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 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.

- 6. 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. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See **Tips for Adding a Web Browser Interface** (on page 149) 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, KSX II 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.

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 157) 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. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See **Tips for Adding a Web Browser Interface** (on page 149) 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, Supported CIMs for Blade Chassis, and **Required and Recommended Blade Chassis Configurations** (on page 155) for important, additional information when configuring the blade chassis. See **Dell Chassis Cable Lengths and Video Resolutions** (on page 315) for information on cable lengths and video resolutions when using Dell® chassis with the KSX II.

► To add a blade chassis:

1. Connect the blade chassis to the KSX II. See Step 3: Connect the Equipment for details.
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). Additionally, a user account with the corresponding authentication credentials must be previously created on the blade chassis. The KSX II 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 KSX II 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 KSX II assigns the chassis a name. The default naming convention for the blade chassis by the KSX II 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.

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 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. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See **Tips for Adding a Web Browser Interface** (on page 149) 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  or the Apply Select Profiles to Other Ports icon  to expand these sections of the page. See **Configuring USB Profiles (Port Page)** (on page 158).
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 KSX II 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.

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 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. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See **Tips for Adding a Web Browser Interface** (on page 149) 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 KSX II 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 KSX II.

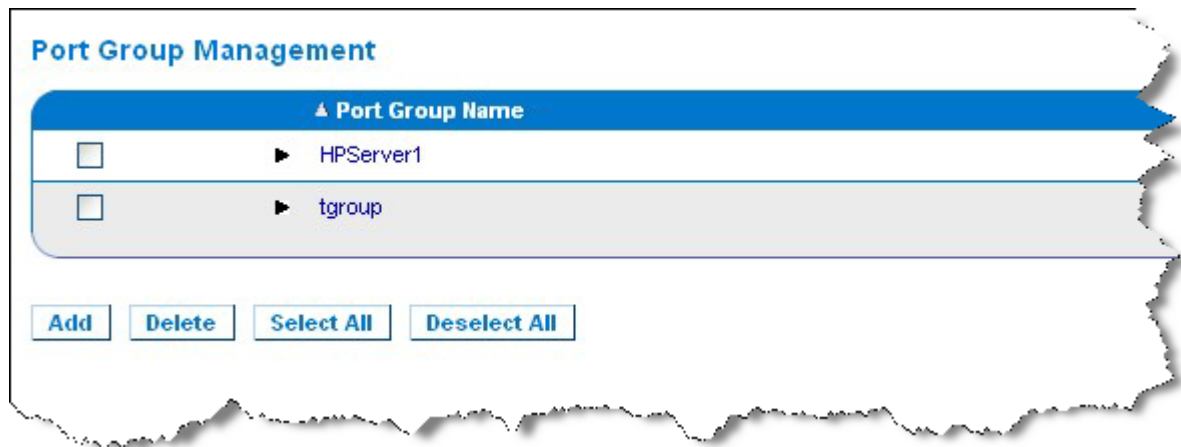
The chassis is identified by a Port Group Name and the group is designated as a Blade Server Group on the Port Group Management page. Port Groups consist solely of ports configured as standard KVM ports, not ports configured as blade chassis. A port may only be a member of a single group.

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 KSX II 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 (see **Backup and Restore** (on page 214)).



► **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 KSX II.

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.

► **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 KSX II and the corresponding profiles that should be selected per chassis model when configuring them in the KSX II 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	KSX II Profile
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 Blade Chassis Configuration (Port Group Management)</i> (see " <i>HP and Cisco UCS Blade Chassis Configuration (Port Group Management)</i> " on page 150).

Supported CIMs for Blade Chassis

The following CIMs are supported for blade chassis being managed through the KSX II:

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

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

Blade chassis	Connection method	Recommended CIM(s)
Generic	If a D2CIM-VUSB or D2CIM-DVUSB is used	<ul style="list-style-type: none"> • DCIM-PS2

Blade chassis	Connection method	Recommended CIM(s)
	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.	<ul style="list-style-type: none"> • DCIM-USBG2
Cisco® UCS Server Chassis	<p>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.</p> <p>Source: <i>Cisco UCS 5108 Server Chassis Installation Guide</i></p>	<ul style="list-style-type: none"> • DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB
Dell® PowerEdge™ 1855	<p>Includes one of the three KVM modules :</p> <ul style="list-style-type: none"> • Analog KVM Ethernet switch module (standard) • Digital Access KVM switch module (optional) • KVM switch module (standard on systems sold prior to April, 2005) <p>These switches provide a custom connector that allows two PS/2 and one video device to be connected to the system.</p> <p>Source: <i>Dell PowerEdge 1855 User Guide</i></p>	<ul style="list-style-type: none"> • DCIM-PS2
Dell PowerEdge 1955	<p>One of two types of KVM modules may be installed:</p> <ul style="list-style-type: none"> • Analog KVM switch module • Digital Access KVM switch module <p>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).</p> <p>Source: <i>Dell PowerEdge 1955 Owner's Manual</i></p>	<ul style="list-style-type: none"> • DCIM-PS2
Dell PowerEdge M1000e	<p>The KVM Switch Module (iKVM) is Integrated with this chassis.</p> <p>The iKVM is compatible with the following peripherals:</p> <ul style="list-style-type: none"> • USB keyboards, USB pointing devices • VGA monitors with DDC support. <p>Source: <i>Dell Chassis Management Controller,</i></p>	<ul style="list-style-type: none"> • DCIM-USBG2

Blade chassis	Connection method	Recommended CIM(s)
	<i>Firmware Version 1.0, User Guide</i>	
HP® BladeSystem c3000	<p>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.</p> <p>Source: <i>HP ProLiant™ BL480c Server Blade Maintenance and Service Guide</i></p>	<ul style="list-style-type: none"> • DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (for standard KVM port operation without a KVM option)
HP BladeSystem c7000	<p>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.</p> <p>Source: <i>HP ProLiant BL480c Server Blade Maintenance and Service Guide</i></p>	<ul style="list-style-type: none"> • DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (for standard KVM port operation)
IBM® BladeCenter® S	<p>The Advanced Management Module (AMM) provides system management functions and keyboard/video/mouse (KVM) multiplexing for all blade chassis.</p> <p>The AMM connections include: a serial port, video connection, remote management port (Ethernet), and two USB v2.0 ports for a keyboard and mouse.</p> <p>Source: <i>Implementing the IBM BladeCenter S Chassis</i></p>	<ul style="list-style-type: none"> • DCIM-USBG2
IBM BladeCenter H	<p>The BladeCenter H chassis ships standard with one Advanced Management Module.</p> <p>Source: <i>IBM BladeCenter Products and Technology</i></p>	<ul style="list-style-type: none"> • DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter E	<p>The current model BladeCenter E chassis (8677-3Rx) ships standard with one Advanced Management Module.</p> <p>Source: <i>IBM BladeCenter Products and Technology</i></p>	<ul style="list-style-type: none"> • DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	<p>The BladeCenter T chassis ships standard with one Advanced Management Module.</p> <p>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</p>	<ul style="list-style-type: none"> • DCIM-PS2

Blade chassis	Connection method	Recommended CIM(s)
	<p>KVM connections are fed through to the rear to the LAN and KVM modules.</p> <p>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.</p> <p>Source: <i>IBM BladeCenter Products and Technology</i></p>	
IBM BladeCenter HT	<p>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.</p> <p>Source: <i>IBM BladeCenter Products and Technology</i></p>	<ul style="list-style-type: none"> • 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 KSX II only supports auto-discovery for AMM[1] as the acting primary management module.

Required and Recommended Blade Chassis Configurations

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

Blade chassis	Required/recommended action
Dell® PowerEdge™ M1000e	<ul style="list-style-type: none"> ▪ 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

Blade chassis	Required/recommended action
	<p>not work correctly otherwise.</p> <ul style="list-style-type: none"> ▪ Designate a single key sequence to invoke the iKVM GUI. This key sequence must also be identified during KSX II 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 KSX II 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	<ul style="list-style-type: none"> ▪ 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, 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	<ul style="list-style-type: none"> ▪ 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 KSX2 Virtual Media	<ul style="list-style-type: none"> ▪ Raritan KSX II virtual media is supported only on IBM BladeCenter® Models H and E. This requires the use of the

Blade chassis	Required/recommended action
	D2CIM-DVUSB. The black D2CIM-DVUSB Low-Speed USB connector is attached to the Administrative Management Module (AMM) at the rear of the unit. The gray D2CIM-DVUSB High-Speed USB connector is attached to the Media Tray (MT) at the front of the unit. This will require a USB extension cable.
Cisco® UCS Server Chassis	<ul style="list-style-type: none"> ▪ 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 KSX II.

Note: In the case of IBM Blade Center Models E and H, the KSX II 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 KSX II.

Blade chassis	Sample URL format
Dell® M1000e	<ul style="list-style-type: none"> • URL: https://192.168.60.44/cgi-bin/webcgi/login • Username: root • Username Field: user • Password: calvin • Password Field: password
Dell 1855	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 92).

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 KSX II. See Upgrading CIMs.

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 99) 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.

Apply	Port Number	Port Name	Selected USB Profiles
<input type="checkbox"/>	3	vm-cim #1	Generic, Troubleshooting 1, Troubleshooting 2, Troubleshooting 3
<input type="checkbox"/>	5	vm-cim #2	CIM firmware upgrade required!
<input checked="" type="checkbox"/>	15	charles_cim - vm-cim #3	Generic, Troubleshooting 1, Troubleshooting 2, Troubleshooting 3

OK Select All Deselect All Cancel

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

Configuring KSX II Local Port Settings

From the Local Port Settings page, you can customize many settings for the KSX II Local Console including keyboard, hot keys, video switching delay, power save mode, local user interface resolution settings, and local user authentication. Further, you can change a USB profile from the local port.

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.
2. 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 will be restarted when this change is made.
3. If needed, configure the Local Port Scan Mode settings. These settings apply to Scan Settings feature, which is accessed from the Port page. See Scanning Ports.
 - 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.
4. 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)
- JIS (Japanese Industry Standard)
- Simplified Chinese
- Traditional Chinese
- Dubeolsik Hangul (Korean)
- German (Switzerland)

- 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 KSX II 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.

5. Choose the local port hotkey. The local port hotkey is used to return to the KSX II 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

6. Select the Local Port Connect key. Use a connect key sequence to connect to a target and switch to another target.

You can then use the hot key to disconnect from the target 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 252) for examples of connect key sequences.

7. The connect key works for both standard servers and blade chassis.
8. Set the Video Switching Delay from between 0 - 5 seconds, if necessary. Generally 0 is used unless more time is needed (certain monitors require more time to switch the video).

9. 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.
10. Choose the resolution for the KSX II Local Console from the drop-down list. The browser will be restarted when this change is made.
 - 800x600
 - 1024x768
 - 1280x1024
11. Choose the refresh rate from the drop-down list. The browser will be restarted when this change is made.
 - 60 Hz
 - 75 Hz
12. Choose the type of local user authentication.
 - Local/LDAP/RADIUS. This is the recommended option. For more information about authentication, see Remote Authentication.
 - None. There is no authentication for Local Console access. This option is recommended for secure environments only.
 - Select the "Ignore CC managed mode on local port" checkbox if you would like local user access to the KSX II even when the device is under CC-SG management.

Note: If you initially choose not to ignore CC Manage mode on the local port but later want local port access, you will have to remove the device from under CC-SG management (from within CC-SG). You will then be able to check this checkbox.

13. Click OK.

Device Services

The Device Services page allows you to configure the following functions:

- Enabling Telnet
- Enabling SSH access
- Configuring HTTP and HTTPs port settings
- Enabling Serial Console Access
- Configuring the discovery port access
- Enabling direct port access
- Enabling the AKC Download Server Certificate Validation feature if you are using AKC
- SNMP Agent Configuration

Enabling Telnet

If you wish to use Telnet to access the KSX II, first access the KSX II from the CLI or a browser.

► **To enable Telnet:**

1. Select Device Settings > Device Services and then select the Enable TELNET Access checkbox.
2. Enter the Telnet port.
3. Click OK.

Once Telnet access is enabled, you can use it to access the KSX II and set up the remaining parameters.

Enabling SSH

Enable SSH access to allow administrators to access the KSX II 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 KSX II. 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.

► **To change the HTTP and/or HTTPS port settings:**

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

The KSX II 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 the KSX II from beyond a firewall, your firewall settings must enable two-way communication through the default Port 5000 or a non-default port configured here.

► **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.

Enabling Serial Console Access

► **To enable serial console access:**

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Select Enable Serial Console Access.
3. Select the baud rate of the device.
4. Click OK.

Enabling Direct Port Access via URL

Direct port access allows users to bypass having to use the device'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`

Or

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

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**.

Direct Port Access URL Syntax for the Active KVM Client (AKC)

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=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=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.

Client=akc is optional unless you are using the AKC client.

If client=akc is not included, the Virtual KVM Client (VKC) is used as the client.

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**.

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.

Configuring Direct Port Access via Telnet, IP Address or SSH

The information in this topic is specific to enabling direct port access for serial targets. Use the Enable Direct Port Access via URL option on the Device Services page to enable direct port access for a KVM/serial port connected to the KSX II. See Enabling Direct Port Access via URL.

► **To configure direct port access:**

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Type the IP address and ports used for SSH and Telnet in the appropriate fields for each serial target.

Note that leaving all three fields blank will disable direct port access for the serial target. To enable direct port access, you must do one of the following:

- Enable global Telnet or SSH access.
- Input a valid IP address or TCP port in at least one of the three fields.

Important: It is not recommended that more than one of these fields is populated.

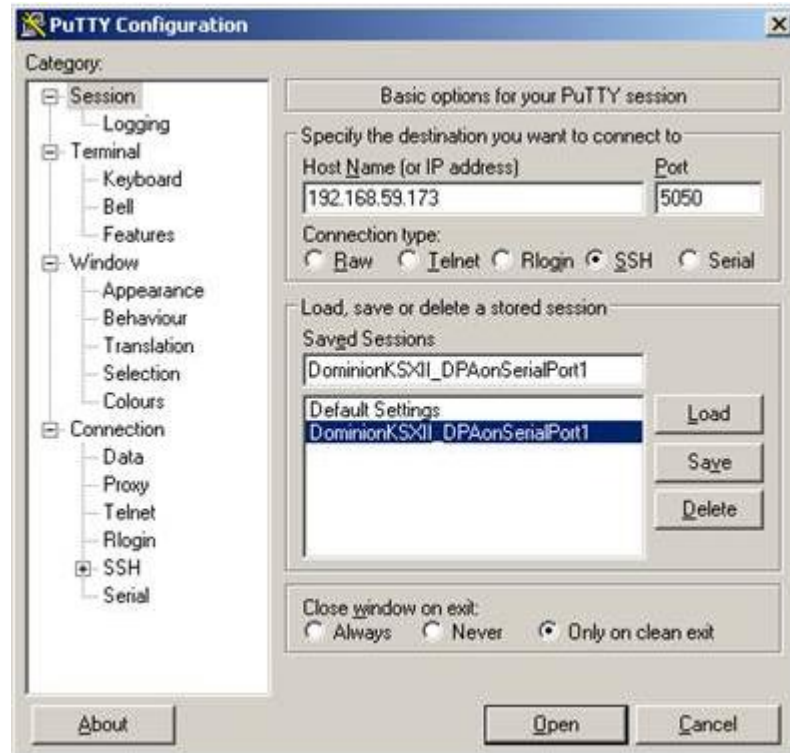
Below are examples of Telnet and IP:

- Direct Port access via IP alias address:
Configure the IP alias address 192.168.1.59 for a serial target. Once this is done, connection to the target through Telnet can be done using "telnet 192.168.1.59".
- Direct Port access via Telnet port:
Configure the Telnet TCP Port as "7770". Once this is done, connection to the target can be done using "telnet <KSX II device IP address> 7770".
- Direct Port Access via SSH Port:
Configure the SSH TCP port as "7888". Once this is done, connection to the target can be done by using "ssh -l <login> <KSX II device IP address> -p 7888".

3. Click OK to save this information.

Direct Port Access				
No.	Name	IP Address	SSH Port	Telnet Port
9	Serial Port 1	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	Serial Port 2	<input type="text"/>	<input type="text"/>	<input type="text"/>
11	Serial Port 3	<input type="text"/>	<input type="text"/>	<input type="text"/>
12	Serial Port 4	<input type="text"/>	<input type="text"/>	<input type="text"/>
13	Serial Port 5	<input type="text"/>	<input type="text"/>	<input type="text"/>
14	Serial Port 6	<input type="text"/>	<input type="text"/>	<input type="text"/>
15	Serial Port 7	<input type="text"/>	<input type="text"/>	<input type="text"/>
16	Serial Port 8	<input type="text"/>	<input type="text"/>	<input type="text"/>

Once you have created the direct port access, it can be connected in a client application such as PuTTY. Following is an example of how the direct port access information would appear in PuTTY. Note that PuTTY is not the only client application that can be used. It is used here for sample purposes only.



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 KSX II IP address in the Trusted Site zone and ensure 'Protected Mode' is off.

2. Launch Internet Explorer® using the KSX II 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 KSX II 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 KSX II 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

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 KSX II MIB** (on page 181) for information on viewing the KSX II MIB.

KSX II 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 configure SNMP agents:**

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:
 - a. System Name - the SNMP agent's name/device name
 - b. System Contact - the contact name related to the device
 - c. System Location - the location of the device

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):
 - a. Community - the device's community string
 - b. Community Type - grant either Read-Only or Read-Write access to the community users

Note: An SNMP community is the group to which devices 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):
 - a. 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.
 - b. Security Name - the username or service account name of the entity communicating with the SNMP agent (up to 32 characters)
 - c. Authentication Protocol - the MD5 or SHA authentication protocol used by the SNMP v3 agent
 - d. Authentication Passphrase - the passphrase required to access the SNMP v3 agent (up to 64 characters)
 - e. Privacy Protocol - if applicable, the AES or DES algorithm used to encrypt PDU and context data
 - f. Privacy Passphrase - the passphrase 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 176) for information on creating SNMP traps and **List of KSX II SNMP Traps** (on page 178) for a list of available KSX II 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 182).

► **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 KSX II and the router that it is attached to fall out of synchronization when the KSX II is rebooted, preventing the reboot completed SNMP trap from being logged.

Configuring Modem Settings

► **To configure modem settings:**

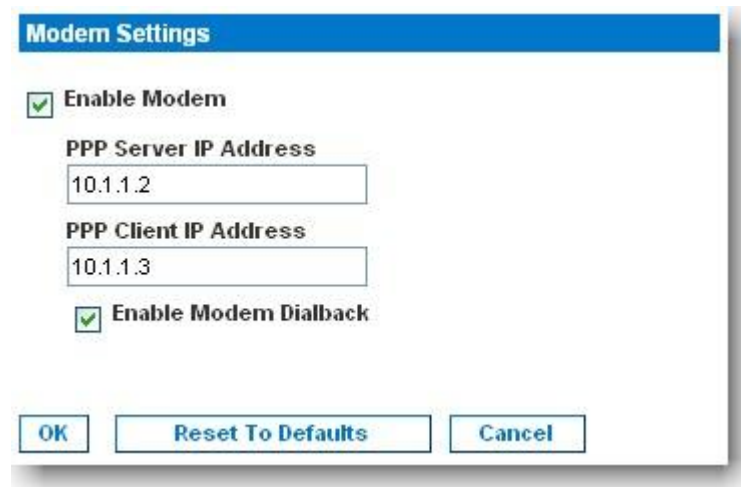
1. Click Device Settings > Modem Settings to open the Modem Settings page.
2. Check Enable Modem, if needed.
3. Enter the PPP server IP address. The internet address assigned to the KSX II when a connection is established via dial-up. **Required**.
4. Enter the PPP client IP address. The internet address the KSX II assigns to remove the client when a connection is established via dial-up. **Required**.

Note: The PPP server IP address and PPP Client IP address must be different and cannot conflict with the network addresses used by the server or the client.

5. Check Enable Modem Dialback, if needed.

Note: If dial-back is enabled, each user accessing the KSX II via modem must have a call-back number defined in their profile. Otherwise, dial-up will reject the call for that user.

6. Click OK to commit your changes or click Reset to Defaults to return the settings to their defaults.



The image shows a 'Modem Settings' dialog box with a blue title bar. It contains the following elements: a checked checkbox for 'Enable Modem', a text field for 'PPP Server IP Address' containing '10.1.1.2', a text field for 'PPP Client IP Address' containing '10.1.1.3', and a checked checkbox for 'Enable Modem Dialback'. At the bottom are three buttons: 'OK', 'Reset To Defaults', and 'Cancel'.

Configuring Date/Time Settings

Use the Date/Time Settings page to specify the date and time for the KSX II. 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 KSX II Event Management feature allows you enable and disable the distribution of system events to SNMP Managers, 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 176).

Once configured, enable the SNMP traps on the Event Management - Destinations page. See **Configuring Event Management - Destinations** (on page 182).

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 KSX II SNMP Traps** (on page 178) for a list of KSX II 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 171) for information on configuring SNMP agents and **Viewing the KSX II MIB** (on page 181) for information on viewing the KSX II MIB.

► To configure SNMP (enable SNMP logging):

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):
 - a. 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.

- b. Port Number - the port number used by the SNMP manager
- c. Community - the device's community string

Note: An SNMP community is the group to which devices 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):

- a. 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.

- b. Port Number - the port number used by the SNMP manager
- c. Security Name - the username or service account name of the entity communicating with the SNMP agent (up to 32 characters)
- d. Authentication Protocol - the MD5 or SHA authentication protocol used by the SNMP v3 agent
- e. Authentication Passphrase - the passphrase required to access the SNMP v3 agent (up to 64 characters)
- f. Privacy Protocol - if applicable, the AES or DES algorithm used to encrypt PDU and context data
- g. Privacy Passphrase - the passphrase 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 KSX II's left panel. See Left Panel

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 182).

KSX II 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.

[Home](#) > [Device Settings](#) > [Event Management - Settings](#)

SNMP Traps Configuration

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

SNMP v1/v2 Trap

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

SNMP v3 Trap

Engine ID: 80001f8803000d5d03ca3b

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

[Link to SNMP Agent Configuration](#)

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

Use the reset to factory defaults feature to remove the SNMP configuration and set the KSX II 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 KSX II and the router that it is attached to fall out of synchronization when the KSX II is rebooted, preventing the reboot completed SNMP trap from being logged.

List of KSX II 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 KSX II SNMP traps:

Trap Name	Description
bladeChassisCommError	A communications error with blade chassis

Trap Name	Description
	device connected to this port was detected.
cimConnected	The CIM is connected.
cimDisconnected	The CIM is disconnected.
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 KSX II has completed update via an RFP file.
deviceUpgradeStarted	The KSX II 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 KSX II 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.

Trap Name	Description
powerOutletNotification	Power strip device outlet status notification.
rebootCompleted	The KSX II has completed its reboot.
rebootStarted	The KSX II 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 KSX II and has been authenticated.
userLogout	A user has successfully logged out of the KSX II 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.
vmImageConnected	User attempted to mount either a device or image on the target using Virtual Media.

Trap Name	Description
	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.

**Note: Not supported by the KX II-101 or LX.*

***Note: FIPS is not supported by the LX.*

Viewing the KSX II MIB

► To view the KSX II MIB:

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens.
2. Click the 'Click here to view the Dominion KSX2SNMP MIB' link. The MIB file opens in a browser window.

Note: If you have Read-Write privileges to the MIB file, use a MIB editor to make changes to the file.

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

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

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

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

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

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

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

SysLog Configuration

► **To configure the Syslog (enable Syslog forwarding):**

1. Select Enable Syslog Forwarding to log the device's messages to a remote Syslog server.
2. Type the IP Address/Hostname of your Syslog server in the IP Address field.
3. Click OK.

Note: IPv6 addresses cannot exceed 80 characters in length for the host name.

Use the reset to defaults feature to remove the syslog configuration.

Configuring Event Management - Destinations

System events, if enabled, generate SNMP notification events (traps), or can be logged to the syslog or audit log. Use the Event Management - Destinations page to select the system events to track and where to send this information.

*Note: SNMP traps are generated only if the SNMP Logging Enabled option is selected. Syslog events are generated only if the Enable Syslog Forwarding option is selected. Both of these options are in the Event Management - Settings page. See **Configuring Event Management - Settings** (on page 175).*

► **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 KSX II and the router that it is attached to fall out of synchronization when the KSX II is rebooted, preventing the reboot completed SNMP trap from being logged.

Connect and Disconnect Scripts

The KSX II 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 KSX II can also be exported in XML file format.

A total of 16 scripts can be accommodated on the KSX II.

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
<input checked="" type="checkbox"/>	5	SE-IX2-232-LP-ChangedName	
<input checked="" type="checkbox"/>	6	Japanese Target	
<input checked="" type="checkbox"/>	8	se-ksx2-188-local-port	On Disconnect: Ctrl-Alt-Del_OnExit
<input checked="" type="checkbox"/>	9	W2K3 Server	
<input checked="" type="checkbox"/>	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 KSX II and import them as XML files. See **Importing and Exporting Scripts** (on page 187).*

► 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

Press F6
Release F6
Press C
Release C

[Add](#) [Remove](#) [^](#) [v](#)

[OK](#) [Cancel](#) [Clear](#)

Home > Device Settings > Connection Scripts > Modify Connection Script

Construct Script From Text

Connected to Target

[OK](#) [Cancel](#) [Clear](#)

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 KSX II 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 184).

► 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 KSX II are not included in the import.
 - Overwrite duplicates - Scripts that already exists in KSX II 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. KSX II 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.

5. Click Import. The Configuration Scripts page opens and the imported scripts are displayed.

Home > Device Settings > Connection Scripts > Import Connection Scripts

Import Connection Scripts

Import Settings

☒ Skip duplicates

☐ Overwrite duplicates

☐ Add duplicates with a different name

Connection Scripts File

► **To export a disconnect script:**

1. Click Device Settings > Configuration Scripts. The Configuration Scripts page opens.
2. 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.
3. 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 Keywords

Port keywords work as a filter. If a keyword is detected, a corresponding message be logged in a local port log and a corresponding trap will be sent via SNMP (if configured).

Defining keywords guarantees that only messages that contain those keywords are logged for the local port.

You can create port keywords and associate them with:

- Syslog
- Audit log
- SNMP traps

► **To define keywords and associate them with a port:**

1. Choose Device Settings > Port Keyword List > Keyword. The Port Keyword List page will open.

Home > Device Settings > Port Keyword List

Port Keyword List			
	Keyword	Port Number	Port Name
<input type="checkbox"/>	panic	9	Cisco 2501
<input type="checkbox"/>	Partial	9	Cisco 2501
<input type="checkbox"/>	question	9	Cisco 2501

If no keywords have been created yet, the page will contain the message *"There are no port keywords defined"*. If port keywords do exist, they will be listed on the Port Keyword List page.

2. Define a keyword for the first time, by clicking the Add button on the Port Keyword List page. The Add Keyword page will then open. Follow steps 3 - 5 to create new keywords.

3. Type a keyword in the Keyword field and then click the Add button. The keyword will be added to the page directly under the Keyword field and will appear on the Port Keyword List page once OK is selected. Add additional keywords by following the same steps (if needed).
4. In the Ports section of the page in the Available selection box, click the port or ports you want to associate with that keyword and click Add. The port associated with the keyword will then be moved to the Selected selection box. Continue adding ports as needed.
5. Click OK.

► **To remove ports from the selected list:**

1. On the Add Keyword page, click the port in the Selected selection box and then click Remove.

► **To delete keywords:**

1. On the Port Keyword List page, check the checkbox of the keyword you would like to delete.
2. Click the Delete button. A warning message will be displayed.
3. Click OK in the warning message.

Port Group Management

This function is specific to HP blade chassis configuration. See ***HP Blade Chassis Configuration (Port Group Management)*** (see "***HP and Cisco UCS Blade Chassis Configuration (Port Group Management)***" on page 150).

Creating Port Groups

The KSX II 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*** (on page 214)).

► 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.

Changing the Default GUI Language Setting

The KSX II GUI defaults to English, but also supports the following localized languages:

- 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.

Chapter 9 Security Management

In This Chapter

Security Settings.....	193
Configuring IP Access Control	204
SSL Certificates	206
Security Banner	209

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 194) settings as appropriate.
3. Update the **Strong Passwords** (on page 196) settings as appropriate.
4. Update the **User Blocking** (on page 197) 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	User Blocking
<input type="checkbox"/> Enable Single Login Limitation <input type="checkbox"/> Enable Password Aging Password Aging Interval (days) <input type="text" value="60"/> <input type="checkbox"/> Log Out Idle Users Idle Timeout (minutes) <input type="text" value="30"/>	<input checked="" type="radio"/> Disabled <input type="radio"/> Timer Lockout Attempts <input type="text" value="3"/> Lockout Time <input type="text" value="5"/> <input type="radio"/> Deactivate User-ID Failed Attempts <input type="text" value="3"/>
Strong Passwords	Encryption & Share
<input type="checkbox"/> Enable Strong Passwords Minimum length of strong password <input type="text" value="8"/> Maximum length of strong password <input type="text" value="16"/> <input checked="" type="checkbox"/> Enforce at least one lower case character <input checked="" type="checkbox"/> Enforce at least one upper case character <input checked="" type="checkbox"/> Enforce at least one numeric character <input checked="" type="checkbox"/> Enforce at least one printable special character Number of restricted passwords based on history <input type="text" value="5"/>	Encryption Mode Auto <input checked="" type="checkbox"/> Apply Encryption Mode to KVM and Virtual Media (Forced in FIPS 140-2 Mode) <input type="checkbox"/> Enable FIPS 140-2 Mode (Changes are activated on reboot only!) Current FIPS status: Inactive PC Share Mode Private <input type="checkbox"/> VM Share Mode Local Device Reset Mode Enable Local Factory Reset
<input type="button" value="OK"/> <input type="button" value="Reset To Defaults"/> <input type="button" value="Cancel"/>	

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 device from several client workstations simultaneously.
Enable password aging	<p>When selected, all users are required to change their passwords periodically based on the number of days specified in Password Aging Interval field.</p> <p>This field is enabled and required when the Enable Password Aging checkbox is selected. Enter the number of days after which a password</p>

Limitation	Description
	change is required. The default is 60 days.
Log out idle users, After (1-365 minutes)	<p>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.</p> <p>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</p>

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 KSX II 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

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

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	<p>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:</p> <ul style="list-style-type: none"> 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. <p><i>Note: Users in the role of Administrator are exempt from the timer lockout settings.</i></p>
Deactivate User-ID	<p>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:</p> <ul style="list-style-type: none"> 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. <p>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.</p>

User Blocking

☒ Disabled

☐ Timer Lockout

Attempts

Lockout Time

☐ Deactivate User-ID

Failed Attempts

Encryption & 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 KSX II 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 KSX II from your browser.

Note that performance may be impacted once encryption is applied. The extent of the performance impact varies based on the encryption mode.

► 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 KSX II.

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 KSX II."

Encryption mode	Description
Auto	<p>This is the recommended option. The KSX II autonegotiates to the highest level of encryption possible.</p> <p>You <i>must</i> select Auto in order for the device and client to successfully negotiate the use of FIPS compliant algorithms.</p>
RC4	<p>Secures user names, passwords and KVM data, including video transmissions using the RSA RC4 encryption method. This is a 128-bit Secure Sockets Layer (SSL) protocol that provides a private communications channel between the KSX II device and the Remote PC during initial connection authentication.</p> <p>If you enable FIPS 140-2 mode and RC4 has been selected, you will receive an error message. RC4 is not available while in FIPS 140-2 mode.</p>
AES-128	<p>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</p>

Encryption mode	Description
	browser supports it, otherwise you will not be able to connect. See Checking Your Browser for AES Encryption (on page 201) 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 201) for more information.

Note: MPC will always negotiate to the highest encryption and will match the Encryption Mode setting if not set to Auto.

Note: If you are running Windows XP® operating system with Service Pack 2, Internet Explorer® 7 cannot connect remotely to the KSX II using AES-128 encryption.

2. Apply Encryption Mode to KVM and Virtual Media. When selected, this option applies the selected encryption mode to both KVM and virtual media. After authentication, KVM and virtual media data is also transferred with 128-bit encryption.
3. 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 202) for information on enabling FIPS 140-2.
4. PC Share Mode - Determines global concurrent remote KVM access, enabling up to eight remote users to simultaneously log into one KSX II 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.
5. 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 among multiple users, that is, several users can access the same virtual media session. The default is disabled.

6. 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 KSX II Using the Reset Button*. Choose one of the following options:

Local device reset mode	Description
Enable Local Factory Reset (default)	Returns the KSX II 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.

Note: When using the P2CIM-AUSBDUAL or P2CIM-APS2DUAL to attach a target to two KSX IIs, if Private access to the targets is required, both KVM switches must have Private set as their PC Share Mode.

See **Supported Paragon CIMS and Configurations** (see "**Supported Paragon II CIMS and Configurations**" on page 282) for additional information on using Paragon CIMS with the KSX II.

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®

In addition to browser support, AES 256-bit encryption requires the installation of Java™ Cryptography Extension® (JCE®) Unlimited Strength Jurisdiction Policy Files.

Jurisdiction files for various JREs™ are available at the "other downloads" section of the following link:

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

Enabling FIPS 140-2

For government and other high security environments, enabling FIPS 140-2 mode may be required.

The KSX II 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 KVM session traffic consisting of video, keyboard, mouse, virtual media and smart card data.

3. Reboot the KSX II. **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 KSX II.

FIPS 140-2 Support Requirements

The KSX II 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 KSX II:

KSX II

- Set the Encryption & Share to Auto on the Security Settings page. See **Encryption & Share** (on page 199).

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.

Configuring IP Access Control

Using IP access control, you control access to your KSX II. Note that IP access control restricts traffic of any kind from accessing the KSX II, so NTP servers, RADIUS hosts, DNS hosts and so on must be granted access to the KSX II.

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 KSX II as a whole, but you can also control access to your device at the group level. See Group-Based IP ACL (Access Control List) for more information about group-level control.

Important: IP address 127.0.0.1 is used by the KSX II 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 KSX II local port.

► **To use IP access control:**

1. Select Security > IP Access Control to open the IP Access Control page.
2. Select the Enable IP Access Control checkbox and the remaining fields on the page.
3. 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 KSX II device.
 - Drop - IP addresses are denied access to the KSX II 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 existing 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 Certificates

The KSX II uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client.

When establishing a connection, the KSX II has to identify itself to a client using a cryptographic certificate.

It is possible to generate a Certificate Signing Request (CSR) and install a certificate signed by the Certificate Authority (CA) on the KSX II.

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 KSX II date/time is set correctly.

When a self-signed certificate is created, the KSX II date and time are used to calculate the validity period. If the KSX II 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 174).

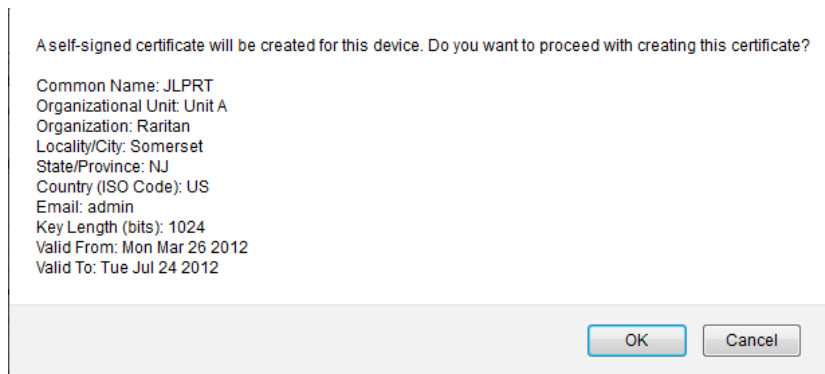
Note: The CSR must be generated on the KSX II.

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 KSX II 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 KSX II 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 KSX II is accessed using HTTPS.
 - b. Organizational unit - This field is used for specifying to which department within an organization the KSX II belongs.
 - c. Organization - The name of the organization to which the KSX II 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. 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.
 - h. Confirm Challenge Password - Confirmation of the Challenge Password. Applicable when generating a CSR for CA Certification.
 - i. Email - The email address of a contact person that is responsible for the KSX II and its security.
 - j. Key length - The length of the generated key in bits. 1024 is the default.
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 KSX II 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 KSX II date and time are correct, otherwise an invalid date may be used to create the certificate's valid from and to range.
 - c. Click Create.
 - d. A confirmation dialog is displayed. Click OK to close it.



- e. Reboot the KSX II 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.

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

- 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 KSX II by clicking Upload.
- Reboot the KSX II to activate the certificate.

After completing these steps the KSX II has its own certificate that is used for identifying the card to its clients.

Important: If you destroy the CSR on the KSX II 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

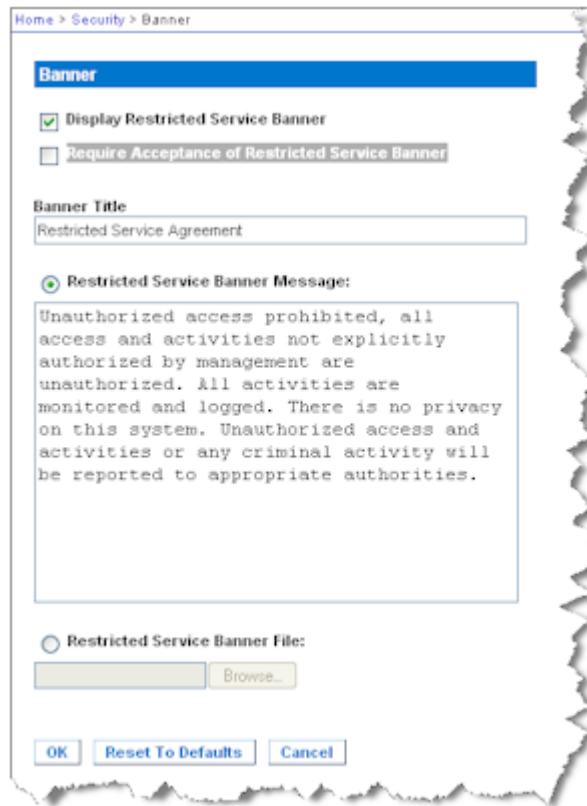
KSX II provides you with the ability to add a security banner to the KSX II login process. This feature requires users to either accept or decline a security agreement before they can access the KSX II. The information provided in a security banner will be displayed in a Restricted Service Agreement dialog after users access KSX II 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 KSX II 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.



The screenshot shows a web interface for configuring a banner. The breadcrumb navigation at the top reads "Home > Security > Banner". The main heading is "Banner". There are two checkboxes: "Display Restricted Service Banner" (checked) and "Require Acceptance of Restricted Service Banner" (unchecked). Below these is a text field for "Banner Title" containing "Restricted Service Agreement". A radio button labeled "Restricted Service Banner Message:" is selected, followed by a large text area containing the 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." Below this is another radio button labeled "Restricted Service Banner File:" which is unselected, followed by a text field and a "Browse..." button. At the bottom are three buttons: "OK", "Reset To Defaults", and "Cancel".

Chapter 10 Maintenance

In This Chapter

Maintenance Features (Local/Remote Console).....	211
Audit Log.....	212
Device Information.....	213
Backup and Restore	214
USB Profile Management	216
Upgrading CIMs.....	217
Upgrading Firmware	217
Upgrade History.....	220
Rebooting the KSX II.....	220
CC Unmanage.....	221

Maintenance Features (Local/Remote Console)

Use:	To:	Local	Remote
Audit Log	View Dominion KSX II events sorted by date and time.	✓	✓
Device Information	View information about the Dominion KSX II and its CIMs.	✓	✓
Backup/Restore	Backup and restore the KSX II configuration.		✓
USB Profile Management	Upload custom profiles provided by Raritan tech support.		✓
CIM Firmware Upgrade	Upgrade your CIMs using the firmware versions stored in the Dominion KSX II memory.	✓	✓
Firmware Upgrade	Upgrade your Dominion KSX II firmware.		✓
Factory Reset	Perform a factory reset.	✓	
Upgrade History	View information about the latest upgrade performed.	✓	✓
Reboot	Reboot the KSX II.	✓	✓

Audit Log

A log is created of the KSX II 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.

► **To view the audit log for your KSX II:**

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 KSX II 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 KSX II device and the CIMs in use. This information is helpful should you need to contact Raritan Technical Support.

► **To view information about your Dominion KSX II and CIMs:**

- Choose Maintenance > Device Information. The Device Information page opens.

The following information is provided about the KSX II:

- 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, Power Strip, or VM)
- Firmware Version
- Serial Number

Device Information	
Model:	DKSX2_188
Hardware Revision:	0x60
Firmware Version:	2.3.0.5.50
Serial Number:	AE17500013
MAC Address:	00:0d:5d:03:5d:0c

CIM Information

Port	Name	Type	Firmware Version	Serial Number
3	Blade_Chassis_Port3	Dual-VM	3A80	PQ20403156

Backup and Restore

From the Backup/Restore page, you can backup and restore the settings and configuration for your KSX II.

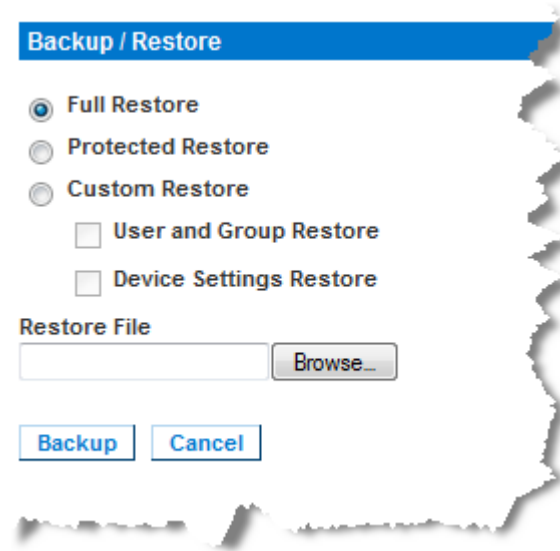
In addition to using backup and restore for business continuity purposes, you can use this feature as a time-saving mechanism.

For instance, you can quickly provide access to your team from another KSX II by backing up the user configuration settings from the KSX II in use and restoring those configurations to the new KSX II.

You can also set up one KSX II and copy its configuration to multiple KSX II devices.

► **To access the Backup/Restore page:**

- Choose Maintenance > Backup/Restore. The Backup/Restore page opens.



The screenshot shows the 'Backup / Restore' page. At the top is a blue header with the text 'Backup / Restore'. Below the header are three radio button options: 'Full Restore' (selected), 'Protected Restore', and 'Custom Restore'. Under 'Custom Restore', there are two checkboxes: 'User and Group Restore' and 'Device Settings Restore'. Below these options is a 'Restore File' section with a text input field and a 'Browse...' button. At the bottom of the form are two buttons: 'Backup' and 'Cancel'.

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 KSX II:**

1. 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®.

2. 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.

► **To restore your KSX II:**

WARNING: Exercise caution when restoring your KSX II 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 KSX II.

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.

1. 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 device-specific information such as IP address, name, and so forth. With this option, you can setup one KSX II and copy the configuration to multiple KSX II devices.
 - 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 KSX II.
 - Device Settings Restore - This option includes only device settings such as power associations, USB profiles, blade chassis related configuration parameters, and Port Group assignments. Use this option to quickly copy the device information.
2. Click Browse. A Choose File dialog appears.
3. Navigate to and select the appropriate backup file and click Open. The selected file is listed in the Restore File field.
4. Click Restore. The configuration (based on the type of restore selected) is restored.

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
<input type="checkbox"/>	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 KSX II:**

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 KSX II:**

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 216) for more information.

Upgrading CIMs

Use this procedure to upgrade CIMs using the firmware versions stored in the memory of your KSX II device. In general, all CIMs are upgraded when you upgrade the device firmware using the Firmware Upgrade page.

► To upgrade CIMs using the KSX II 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.
4. Click OK to continue the upgrade. Progress bars are displayed during the upgrade. Upgrading takes approximately 2 minutes or less per CIM.

Upgrading Firmware

Use the Firmware Upgrade page to upgrade the firmware for your KSX II and all attached CIMs. This page is available in the KSX II Remote Console only.

Important: Do not turn off your KSX II or disconnect CIMs while the upgrade is in progress - doing so will likely result in damage to the device or CIMs.

► **To upgrade your KSX II:**

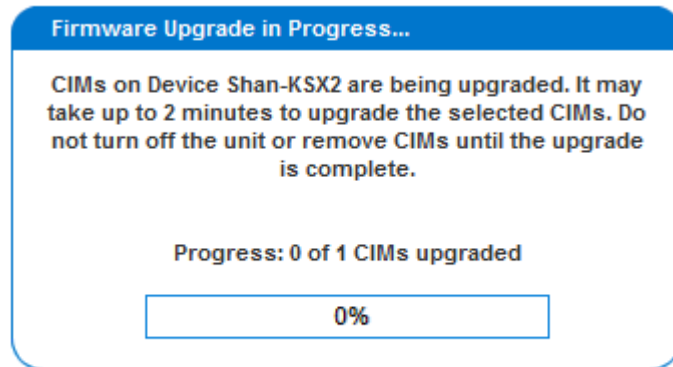
1. Locate the appropriate Raritan firmware distribution file (*.RFP), found on the Raritan Firmware Upgrades webpage: <http://www.raritan.com/support/firmwareupgrades> and download the file.
2. Unzip the file. Read all instructions included in the firmware ZIP files carefully before upgrading.
3. Copy the firmware update file to a local PC before uploading. Do not load the file from a network drive.
4. Choose Maintenance > Firmware Upgrade. The Firmware Upgrade page opens.



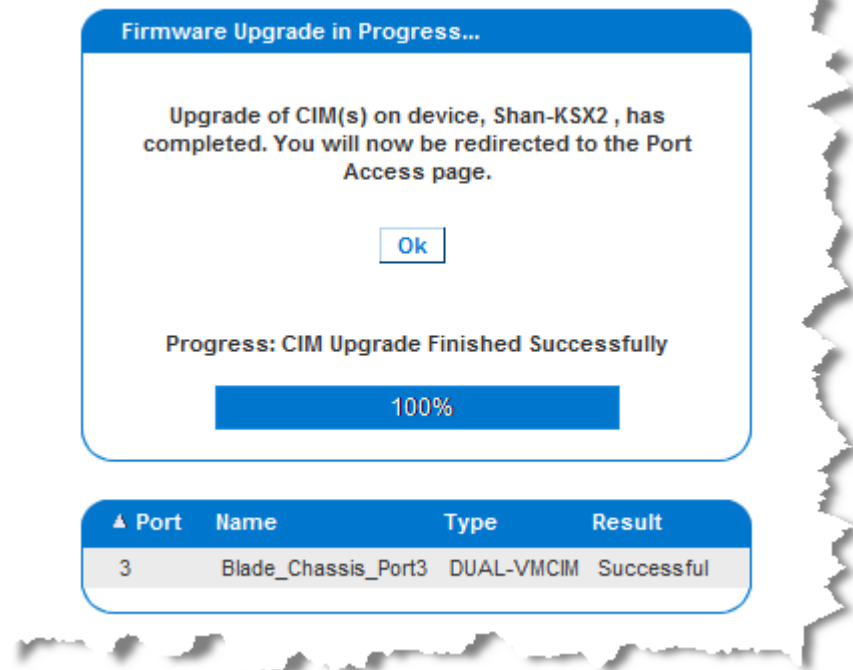
5. Click the Browse button to navigate to the directory where you unzipped the upgrade file.
6. Select the "Review CIM Version Information?" checkbox if you would like information displayed about the versions of the CIMs in use.
7. Click Upload from the Firmware Upgrade page. Information about the upgrade and version numbers is displayed (if you opted to review CIM information, that information is displayed as well).

Note: At this point, connected users are logged off and new login attempts are blocked.

8. Click Upgrade and wait for the upgrade to complete. Status information and progress bars are displayed during the upgrade. Upon completion of the upgrade, the device reboots (1 beep sounds to signal the reboot).



9. As prompted, close the browser and wait approximately 5 minutes before logging on to the KSX II again.



Upgrade History

The KSX II provides information about upgrades performed on the KSX II and attached CIMS.

► **To view the upgrade history:**

- Choose Maintenance > Upgrade History. The Upgrade History page opens.

Type	User	IP	Start Time	End Time	Previous Version	Upgrade Version	CIM's Result
Full Firmware Upgrade	admin	192.168.59.105	October 22, 2007 10:14	October 22, 2007 10:21	1.0.0.1.6127	1.0.0.2.6178	show Successful
Full Firmware Upgrade	admin	192.168.59.124	October 10, 2007 15:55	October 10, 2007 16:02	1.0.0.1.9999	1.0.0.1.6127	show Successful

Information is provided about the KSX II 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:

- Port - The port where the CIM is connected.
- Name - The name of the CIM.
- Type - The type of CIM.
- Previous Version - Previous version of the CIM.
- Upgrade Version - Current version of the CIM.
- Result - The result of the upgrade (success or fail).
-

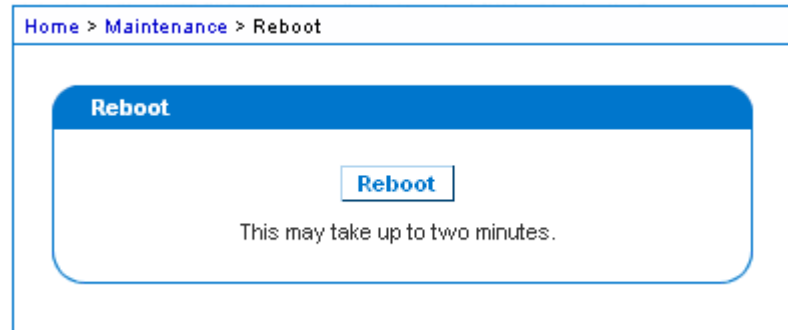
Rebooting the KSX II

The Reboot page provides a safe and controlled way to reboot your KSX II. This is the recommended method for rebooting.

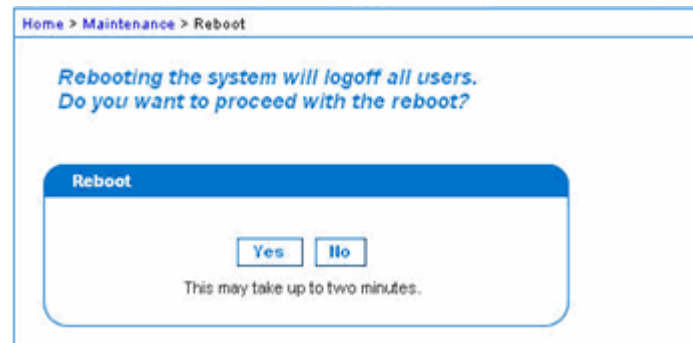
Important: All KVM and serial connections will be closed and all users will be logged off.

► **To reboot your KSX II:**

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.



CC Unmanage

When a KSX II device is under CommandCenter Secure Gateway control and you attempt to access the device directly using the KSX II Remote Console, the following message appears (after entry of a valid user name and password).



Stopping CC-SG Management

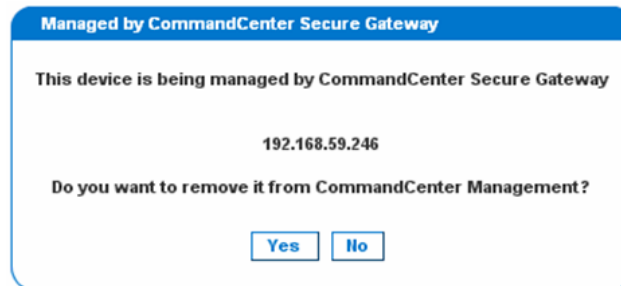
While the KSX II is under CC-SG management, if you try to access the device directly, you are notified that it the device is under CC-SG management.

If you are managing the KSX II through CC-SG and connectivity between CC-SG and the KSX II is lost after the specified timeout interval (typically 10 minutes), you are able to end the CC-SG management session from the KSX II console.

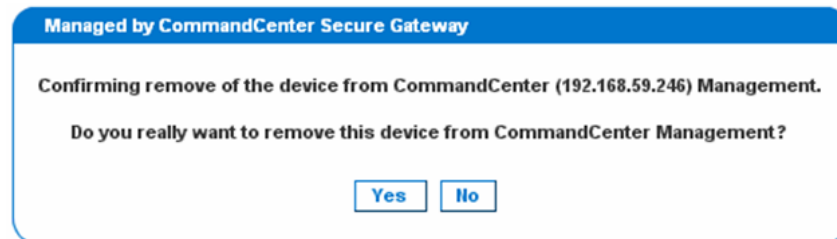
Note: You must have the appropriate permissions to end CC-SG management of the KSX II. Additionally, the Stop CC-SG Management option will not be provided unless you are currently using CC-SG to manage the KSX II.

► To stop CC-SG management of the KSX II:

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 processing of removing the device from CC-SG management. A confirmation message will then displayed asking you to confirm that you want the remove the device from CC-SG management.



3. Click Yes to remove the device CC-SG management. Once CC-SG management has ended, a confirmation will be displayed.



Chapter 11 Diagnostics

The Diagnostics pages are used for troubleshooting and are intended primarily for the administrator of the KSX II device. All of the Diagnostics pages (except Device Diagnostics) run standard networking commands and the information that is displayed is the output of those commands. The Diagnostics menu options help you debug and configure the network settings.

The Device Diagnostics option is intended for use in conjunction with Raritan Technical Support.

In This Chapter

Network Interface Page	224
Network Statistics Page.....	224
Ping Host Page.....	226
Trace Route to Host Page	227
Device Diagnostics	228

Network Interface Page

The KSX II 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 KSX II provides statistics about your network interface.

► **To view 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:

- Statistics - Produces a page similar to the one displayed here.

Home > Diagnostics > Network Statistics

Network Statistics

Options:

Result:

```

Ip:
8803 total packets received
0 forwarded
0 incoming packets discarded
8802 incoming packets delivered
8522 requests sent out
Icmp:
0 ICMP messages received
0 input ICMP message failed.
ICMP input histogram:
0 ICMP messages sent
0 ICMP messages failed
ICMP output histogram:
Tcp:
6 active connections openings
849 passive connection openings
0 failed connection attempts
15 connection resets received
1 connections established
7942 segments received
8304 segments send out
0 segments retransmited
0 bad segments received.
0 resets sent
Udp:
233 packets received
  
```

- 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
eth1 1500 0 13828 0 0 0 8680 0 0 0 BMRU
lo 16436 0 196 0 0 0 196 0 0 0 LRU
  
```

- Route - Produces a page similar to the one displayed here.

Home > Diagnostics > Network Statistics

Network Statistics

Options:

Result:

```

Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
192.168.59.0 * 255.255.255.0 U 0 0 0 eth1
default 192.168.59.126 0.0.0.0 UG 0 0 0 eth1
    
```

3. Click Refresh. The relevant information is displayed in the Result field.

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 KSX II is accessible.

► To ping the host:

1. Choose Diagnostics > Ping Host. The Ping Host page opens.

Home > Diagnostics > Ping Host

Ping Host

Hostname or IP Address:

Result:

```

192.168.59.97 is alive!
    
```

2. Type either the hostname or IP address into the Hostname or IP Address field.
3. Click Ping. The results of the ping are displayed in the Result field.

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.

Home > Diagnostics > Trace Route to Host

Trace Route to Host

IP Address/Host Name
192.168.59.173

Maximum Hops:
10

[Trace Route](#)

Result:

```
tracert started wait for 2mins....
tracert to 192.168.59.173 (192.168.59.173), 10 hops max, 40 byte packets
1 192.168.59.173 (192.168.59.173) 0.497 ms 0.308 ms 0.323 ms
```

Device Diagnostics

Note: This page is for use by Raritan field engineers or when you are directed by Raritan Technical Support.

Device Diagnostics downloads the diagnostics information from KSX II to the client machine. Two operations can be performed on this page:

Operation	Description
Diagnostics Scripts	Execute a special script provided by Raritan Technical Support during a critical error debugging session. The script is uploaded to the device and executed. Once this script has been executed, you can download the diagnostics messages through the Save to File button.
Device Diagnostic Log	Download the snapshot of diagnostics messages from the KSX II 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.

► To run the KSX II system diagnostics:

1. Choose Diagnostics > Device Diagnostics. The Device Diagnostics page opens.
2. To execute a diagnostics script file emailed to you from Raritan Technical Support:
 - a. Retrieve the diagnostics file supplied by Raritan and unzip as necessary.
 - b. Use the Browse button. A Choose File dialog appears.
 - c. Navigate to and select this diagnostics file.
 - d. Click Open. The file is displayed in the Script File field:

Diagnostics Scripts:

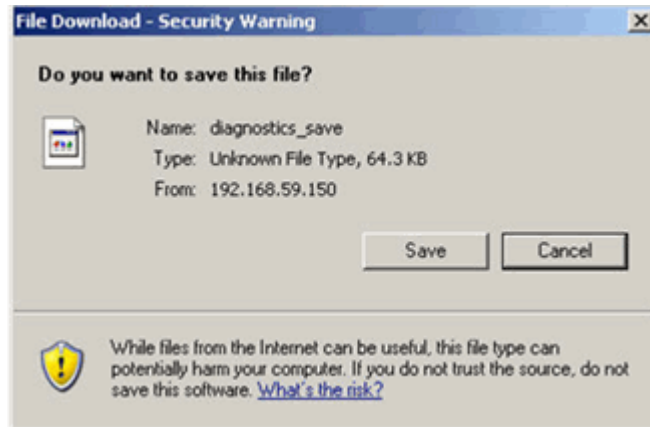
Script File:

C:\Documents and Settings\... Browse...

Run Script Cancel

- e. Click Run Script.

- f. Send this file to Raritan Technical Support using step 4.
3. To create a diagnostics file to send to Raritan Technical Support:
 - a. Click the Save to File button. The File Download dialog appears.



- b. Click Save. The Save As dialog appears.
 - c. Navigate to the desired directory and click Save.
4. Email this file as directed by Raritan Technical Support.

Chapter 12 Command Line Interface (CLI)

In This Chapter

Overview	231
Accessing the KSX II Using CLI	232
SSH Connection to the KSX II	232
Telnet Connection to the KSX II	233
Local Serial Port Connection to the KSX II	233
Logging On	234
Navigation of the CLI	236
Initial Configuration Using CLI	238
CLI Prompts	239
CLI Commands	239
Target Connections and the CLI	240
Administering the KSX II Console Server Configuration Commands ...	241
Configuring Network	241

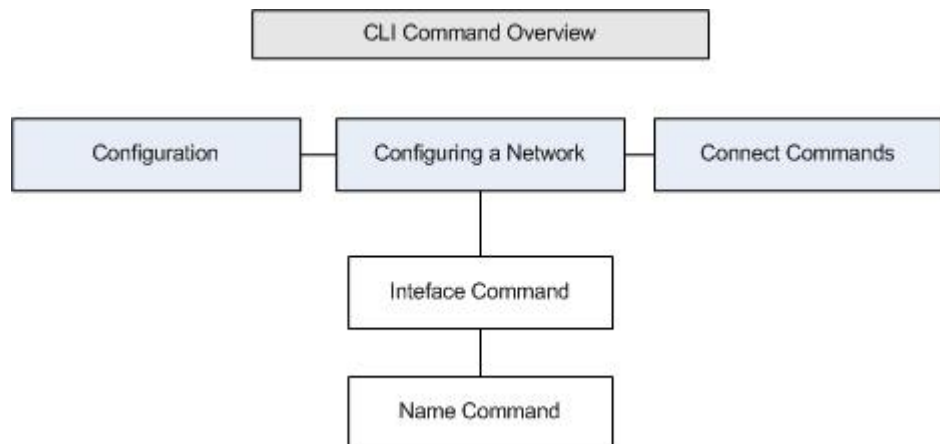
Overview

The KSX II Serial Console supports all serial devices such as:

- Servers, including Windows Server 2003® when using the Emergency Management Console (EMS-) Special Administration Console, or SAC with BIOS redirection in the server BIOS.
- Routers
- Layer 2 switches
- Firewalls
- Rack PDUs (power strips)
- Other user equipment

The KSX II allows an administrator or user to access, control, and manage multiple serial devices. You can use the Command Line Interface (CLI) to configure the KSX II or to connect to target devices. The RS-232 interface may operate at all standard rates from 1200 bps to 115.2 kbps. The default settings are 9600 bps, 8 data bits, no parity bit, one stop bit, and no flow control.

The following figures describe an overview of the CLI commands. See **CLI Commands** (on page 239) for a list of all the commands, which include definitions and links to the sections in this chapter that give examples of these commands.



The following common commands can be used from all levels of the CLI to the preceding figure: top, history, log off, quit, show, and help.

Accessing the KSX II Using CLI

Access the KSX II by using one of the following methods:

- Telnet via IP connection
- SSH (Secure Shell) via IP connection
- Local Port-via RS-232 serial interface

A number of SSH/Telnet 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.netbeans.org/ssh
<http://www.netbeans.org/ssh>
- OpenSSH Client - www.openssh.org <http://www.openssh.org>

SSH Connection to the KSX II

Use any SSH client that supports SSHv2 to connect to the KSX II. You must enable SSH access from the Devices Services page.

Note: For security reasons, SSH V1 connections are not supported by the KSX II.

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 KSX II server. For example, 192.168.0.192.
3. Choose SSH, which uses the default configuration port 22.
4. Click Open.
5. The `login as:` prompt appears.

SSH Access from a UNIX/Linux Workstation

► **To open an SSH session from a UNIX®/Linux® workstation and log in as the user admin, enter the following command:**

```
ssh -l admin 192.168.30.222
```

The Password prompt appears.

Telnet Connection to the KSX II

Due to the lack of security, user name, password and all traffic is in clear-text on the wire. Telnet access is disabled by default.

Enabling Telnet

If you wish to use Telnet to access the KSX II, first access the KSX II from the CLI or a browser.

► **To enable Telnet:**

1. Select Device Settings > Device Services and then select the Enable TELNET Access checkbox.
2. Enter the Telnet port.
3. Click OK.

Once Telnet access is enabled, you can use it to access the KSX II and set up the remaining parameters.

Accessing Telnet from a Windows PC

► **To open a Telnet session from a Windows® PC:**

1. Choose Startup > Run.
2. Type *Telnet* in the Open text box.
3. Click OK. The Telnet page opens.
4. At the prompt enter the following command: `Microsoft Telnet> open <IP address>` where <IP address> is the KSX II IP address.
5. Press the Enter key. The following message appears: `Connecting To <IP address>... The login as prompt appears.`

Local Serial Port Connection to the KSX II

The local serial port of the KSX II must be connected to the COM port of a computer system, a terminal, or some other serial capable device using a null modem cable with DB-9F null on both ends.

If your KSX II's terminal port uses an RJ45 jack, a special cable (CRLVR) is used with an ASCSDB9F connector on the client machine. The CRLVR may also be used if RJ45-RJ45 connection to local port is established - that is, if you connect the local port of an KSX II as a serial target to another KSX II.

Port Settings

Ensure that the port settings (serial communication parameters) are configured as follows:

- Data bits = 8
- Parity = None
- Stop bits = 1
- Flow Control = None
- Bits per second = 9600

Logging On

► **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** (on page 236) section, perform the Initial Configuration tasks.

```
Welcome!

192.168.59.202 login: admin

Passwd:
-----
-----

Device Type: Dominion KSX2      Model: DKSX2_188
Device Name: YongKSX2          FW Version: 1.0.0.5.6321
SN: AE17950009

IP Address: 192.168.59.202      Idle Timeout: 0min
IP Address: 192.168.59.202      Idle Timeout: 0min

Port Port          Port          Port  Port
No.  Name          Type          Status
Availability

1 - Dominion_KSX2_Port1 Not Available down  idle
2 - Dominion_KSX2_Port3 Not Available down  idle
3 - Dominion_KSX2_Port4 Not Available down  idle
4 - Dominion_KSX2_Port5 Not Available down  idle
5 - YongFedora7        VM          up    idle
6 - Yong-Laptop-XP     Not Available down  idle
7 - Dominion_KSX2_Port8 Not Available down  idle
8 - Serial Port 1      Serial      up    idle
9 - Serial Port 2      Serial      up    idle
10 - Serial Port 3     Serial      up    idle
11 - Serial Port 4     Serial      up    idle
12 - Serial Port 5     Serial      up    idle
13 - Serial Port 6     Serial      up    idle
14 - Serial Port 7     Serial      up    idle
15 - Serial Port 8     Serial      up    idle

Current Time: Tue Dec 04 13:22:17 2007

admin >
```

```
login as: Janet
Password:
Authentication successful.

-----
-----

Welcome to the KSX II  [Model: KSX2]

UnitName:KSX II      FirmwareVersion:3.0.0.5.1
Serial:WACEA00008

IP Address:192.168.51.194  UserIdletimeout:99min

-----
-----

Port  Port                Port  Port
No.   Name                No.   Name
1  -  Port1 [U]           2  -  Port2 [U]
3  -  Port3 [U]           4  -  Port4 [U]

Current Time: Wed Sep 20 16:05:50 2006
Janet >
```

Navigation of 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 single word without 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 KSX II 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 for more information.

KSX II 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 KSX II 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 KSX II 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. At the top level, you will see the "Username" > prompt, which for the initial configuration is "admin". Enter the top command to return to the top menu level.

Note: If you have logged on with a different user name, that user name will appear instead of admin.

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 KSX II will need to be reset to the factory default from the Reset button on the back of the KSX II. The initial configuration tasks will need to be performed again if this is done.

The KSX II 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 KSX II.

CLI Prompts

The Command Line Interface prompt indicates the current command level. The root portion of the prompt is the login name. For a direct admin serial port connection with a terminal emulation application, Admin Port is the root portion of a command.

```
admin >
```

For Telnet/SSH, admin is the root portion of the command:

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

0

CLI Commands

The table below lists and describes all available CLI commands.

Command	Description
config	Port configuration command Switch to the Configuration menu.
connect	Connect to a port.
diagnostics	Switch to diagnostic commands menu.
help	Display an overview of the CLI syntax.
history	Display the current session's command line history.
interface	Configure the KSX II network interface.
listports	List accessible ports.
logout	Logout of the current CLI session.
name	Display or change a device name and/or the hostname.
quit	Return to previous command
userlist	List users.

Security Issues

Elements to consider when addressing security for console servers:

- Encrypting the data traffic sent between the operator console and the KSX II device.
- Providing authentication and authorization for users.
- Security profile.

The KSX II supports each of these elements; however, they must be configured prior to general use.

Target Connections and the CLI

The purpose of the KSX II is to let authorized users establish connections to various targeted devices using the connect command. Before connecting to a target, the terminal emulation and escape sequence must be configured. When a target is disconnected, the appropriate disconnect message appears. The KSX II also provides the ability to share ports among users.

Setting Emulation on a Target

► **To set emulation on the target:**

- Ensure that the encoding in use on the host matches the encoding configured for the target device, that is, if the character-set setting on a Sun™ Solaris™ server is set to ISO8859-1, the target device should also be set to ISO8859-1.

Note: ISO9660 format is the standard supported by Raritan. However, other CD-ROM extensions may also work.

- Ensure that the terminal emulation on the target host connected to the KSX II serial port is set to VT100, VT220, VT320 or ANSI.

On most UNIX® systems, export TERM=vt100 (or vt220|vt320|ansi)” sets the preferred terminal emulation type on the UNIX target device, that is, if the terminal type setting on a HP-UX® server is set to VT100, the Access Client should also be set to VT100.

The setting for terminal emulation on the KSX II is a property associated with the port settings for a particular target device. Ensure that the settings for terminal emulation in the client software such as Telnet or SSH client are capable of supporting the target device.

Port Sharing Using CLI

It is possible for access client users to share ports with other authenticated and authorized users, regardless of whether they are access client users (RSC) or SSH/Telnet users. Port sharing is used for training or for troubleshooting applications.

- Users are notified in real time if they have Write access or Read-Only access at any point during the port-sharing session.
- Users who have Write permissions can request Write access to a port.

Administering the KSX II Console Server Configuration Commands

Note: CLI commands are the same for SSH, Telnet, and Local Port access sessions.

The Network command can be accessed in the Configuration menu for the KSX II.

Configuring Network

The network menu commands are used to configure the KSX II network adapter.

Commands	Description
interface	Configure the KSX II device network interface.
name	Network name configuration
ipv6	Set/get IPv6 network parameters.

Interface Command

The Interface command is used to configure the KSX II 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 network name. 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 network name:

```
Admin > Config > Network > name devicename My-KSX2
```

Connect Commands

The connect commands provide a means to access ports and their history.

Command	Description
connect	Connect to a port. The port sub-menu, reached using escape key sequence.
clearhistory	Clear history buffer for this port. Only available to users who have Write access.
clientlist	Display all users on the port.
close	Close this target connection.
gethistory	Display the history buffer for this port. Not available to users who only have Read-Only permissions.
getwrite	Get write access for the port. Not available to users who only have Read-Only permissions.
help	Display an overview of the commands.
history	Display the current session's command line history.
powerstatus	Quersy the Power Status port. Not available to users who do not have power permission.
powertoggle	Toggle power on and off for the port. Not available to users who do not have power permission. Operational for power associated serial targets only.
quit	Close this target connection.
return	Return to the target session.
sendbreak	Send a break to the connected target. Not available to users who only have Read-Only permissions.
writelock	Lock write access to this port. Not available to users who only have Read-Only permissions.
writeunlock	Unlock write access to this port. Not available to users who only have Read-Only permissions.

IPv6 Command

Use the IPv6_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
```

Chapter 13 KSX II Local Console

In This Chapter

Overview	245
Using the KSX II Local Console	245
KSX II Local Console Interface	246
Security and Authentication	246
Available Resolutions	247
Port Access Page (Local Console Server Display)	247
Accessing a Target Server	247
Scanning Ports - Local Console	248
Local Console Smart Card Access	249
Local Console USB Profile Options	250
Server Display	251
Hot Keys and Connect Keys	252
KSX II Supported Keyboard Languages	254
Special Sun Key Combinations	255
Returning to the KSX II Local Console Interface	255
Local Port Administration	256
Resetting the KSX II Using the Reset Button	260

Overview

The KSX II provides at-the-rack access and administration via its local port, which features a browser-based graphical user interface for quick, convenient switching between servers. The KSX II Local Console provides a direct analog connection to your connected servers; the performance is as if you were directly connected to the server's keyboard, mouse, and video ports. The KSX II Local Console provides the same administrative functionality as the KSX II Remote Console.

Using the KSX II Local Console

Simultaneous Users

The KSX II Local Console provides an independent access path to the connected KVM target servers. For serial connections, the access path is shared. Using the Local Console does not prevent other users from simultaneously connecting over the network. And even when remote users are connected to KSX II, you can still simultaneously access your servers from the rack via the Local Console.

KSX II Local Console Interface

When you are located at the server rack, the KSX II provides standard KVM management and administration via the KSX II Local Console. The KSX II Local Console provides a direct KVM (analog) connection to your connected servers; the performance is exactly as if you were directly connected to the server's keyboard, mouse, and video ports. Additionally, the KSX II provides terminal emulation when accessing serial targets.

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

The KSX II Local Console Factory Reset option is available in the KSX II Local Console but not the KSX II Remote Console.

Security and Authentication

In order to use the KSX II Local Console, you must first authenticate with a valid username and password. The KSX II provides a fully-integrated authentication and security scheme, whether your access is via the network or the local port. In either case, the KSX II allows access only to those servers to which a user has access permissions. See User Management for additional information on specifying server access and security settings.

If your KSX II 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 KSX II Local Console:**

1. Connect a keyboard, mouse, and video display to the local ports at the back of the KSX II.
2. Start the KSX II. The KSX II Local Console interface displays.

Available Resolutions

The KSX II Local Console provides the following resolutions to support various monitors:

- 800x600
- 1024x768
- 1280x1024

Each of these resolutions supports a refresh rate of 60Hz and 75Hz.

Port Access Page (Local Console Server Display)

After you login to the KSX II Local Console, the Port Access page opens. This page lists all of the KSX II ports, and the target servers, port groups, and blade chassis that are connected to those ports.

The Port Access page contains the same information whether accessed from the remote console or local console. Additionally, you navigate the page and access targets and port groups in the same way. See Port Access Page (Remote Console Display) for details.

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.

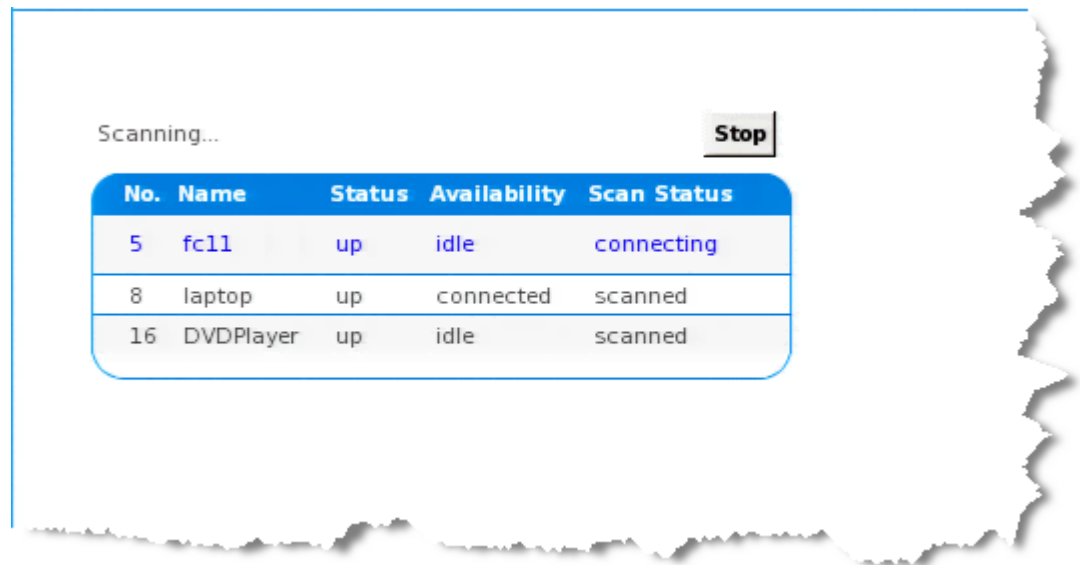
Scanning Ports - Local Console

The KSX II scanning feature is supported by the Local Console.

The targets that are found during the scan are displayed on the Scan page one at a time, which is different from the Remote Console port slide show.

Each target is displayed on the page for 10 seconds by default, allowing you to view the target and connect to it.

Use the Local Port ConnectKey sequence to connect to a target when it is displayed and the DisconnectKey sequence to disconnect from the target.



► **To scan for targets:**

1. From the Local Console, 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. A Port Scan window opens. As each target is found, it is displayed in the window.
5. Connect to a target when it is displayed by using the ConnectKey sequence.

6. Click Stop Scan to stop the scan.

Local Port Scan Mode

Following are options available to you to change scan options on local port.

► **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.

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 KSX II using one of the USB ports located on the KSX II.

Once a smart card reader is plugged in or unplugged from the KSX II, the KSX II autodetects it.

For a list of supported smart cards and additional system requirements, see **Supported and Unsupported Smart Card Readers** (on page 292) and **Smart Card Minimum System Requirements** (on page 290).

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.

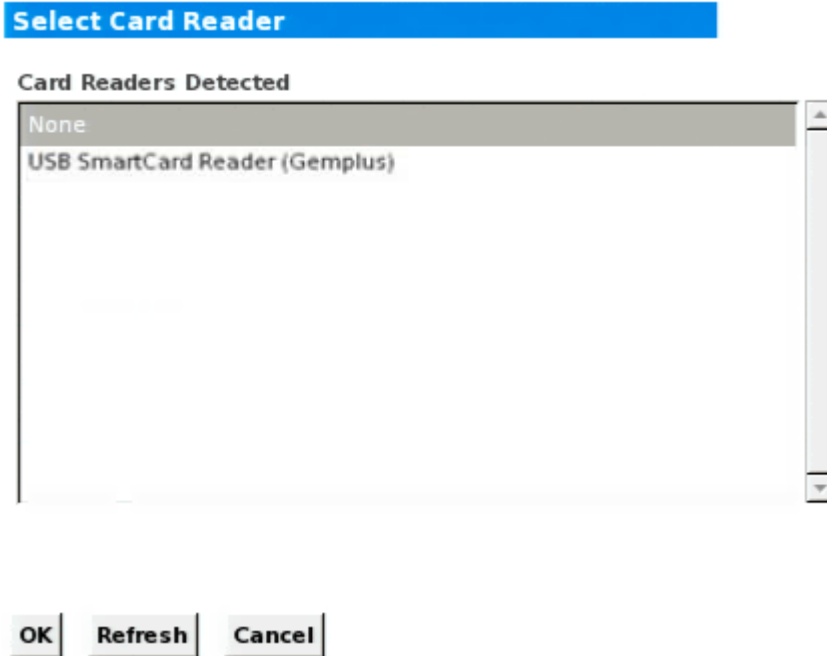
► **To mount a smart card reader onto a target via the KSX II Local console:**

1. Plug a USB smart card reader into the KSX II using one of the USB ports located on the device. Once attached, the smart card reader will be detected by the KSX II.
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

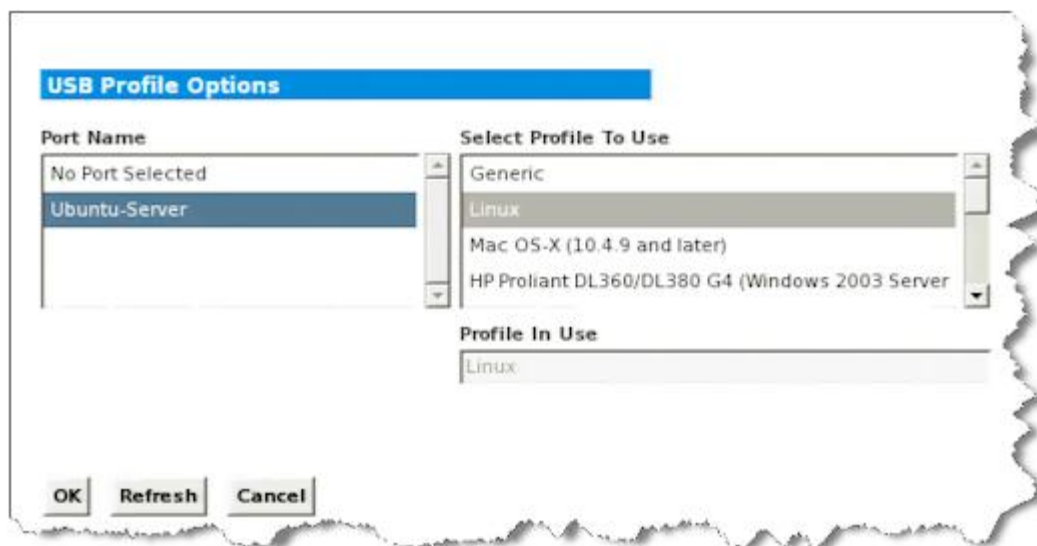
From the USB Profile Options section of the Tools page, you can choose from the available USB profiles.

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.

- Click OK. The USB profile will be applied to the local port and will appear in the Profile In Use field.



Server Display

After you login to the KSX II Local Console, the Port Access page opens. This page lists all of the KSX II ports, KVM target servers and serial servers, and their status and availability.

Port Access

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

Port Number	Port Name	Port Type	Status	Availability
1	Win Target	VM	up	idle
2	Dominion_KSX2_Port2	Not Available	down	idle
3	Dominion_KSX2_Port3	Not Available	down	idle
4	KSX-G2 Admin	VM	up	idle
5	Dominion_KSX2_Port5	Not Available	down	idle
6	Dominion_KSX2_Port6	Not Available	down	idle
7	Dominion_KSX2_Port7	Not Available	down	idle
8	Dominion_KSX2_Port8	Not Available	down	idle
9	Cisco 2501	Serial	up	idle
10	SP-2	Serial	up	idle
11	Serial Port 3	Serial	up	idle
12	Serial Port 4	Serial	up	idle
13	SP - 5	Serial	up	idle
14	Serial Port 6	Serial	up	idle
15	Serial Port 7	Serial	up	idle
16	Serial Port 8	Serial	up	idle

The KVM and serial target servers are initially sorted by Port Number; you can change the display to sort on any of the columns.

- Port Number - Numbered from 1 to the total number of ports available for the KSX II.
- Port Name - The name of the KSX II port. Initially this is set to Dominion-KSX II-Port#, but you can change the name to something more descriptive. When you click the Port Name link, an Action Menu is opened.
- Port Type - Serial, KVM, Power Strip, or Not Available.

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

- Status - The Status is either up or down.

► **To change the sort order:**

- Click the column heading you want to sort by. The list of KVM target servers is sorted by that column.

Hot Keys and Connect Keys

Because the KSX II Local Console interface is completely replaced by the interface for the target server 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 KSX II Local Console user interface when a target server is currently being viewed.

See [Configuring KSX II Local Console Local Port Settings](#) for more information.

Connect Key Examples

Standard servers

Connect key action	Key sequence example
Access a port from the local port GUI	Access port 5 from the local port GUI: <ul style="list-style-type: none"> • Press Left ALT > Press and Release 5 > Release Left ALT
Switch between ports	Switch from target port 5 to port 11: <ul style="list-style-type: none"> • Press Left ALT > Press and Release 1 > Press and Release 1 > Release Left ALT
Disconnect from a target and return to the local port GUI	Disconnect from target port 11 and return to the local port GUI (the page from which you connected to target):

Standard servers	
Connect key action	Key sequence example
	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 the local port GUI	Disconnect from target port 5, slot 11 and return to the local port GUI (the page from which you connected to target): <ul style="list-style-type: none"> Double Click Scroll Lock

KSX II Supported Keyboard Languages

The KSX II 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 KSX II Local Console functions. For more information about non-US keyboards, see Informational Notes.

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 Traditional	Hong Kong S. A. R., Republic of China (Taiwan)	Chinese Traditional
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

Language	Regions	Keyboard layout
Spanish	Spain and most Spanish speaking countries	Spanish
Portuguese	Portugal	Portuguese

Special Sun Key Combinations

The following key combinations for Sun™ Microsystems server's special keys operate on the local port. These special are available from the Keyboard menu when you connect to a Sun target server:

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

Returning to the KSX II Local Console Interface

Important: The KSX II Local Console default hot key is to press the Scroll Lock key twice rapidly.

This key combination can be changed in the Local Port Settings

page. See Configuring KSX II Local Port Settings from the Local Console in online help.

► **To return to the KSX II Local Console from the target server:**

- Press the hot key twice rapidly (the default hot key is Scroll Lock).
The video display switches from the target server interface to the KSX II Local Console interface.

Local Port Administration

The KSX II can be managed by either the KSX II Local Console or the KSX II Remote Console. Note that the KSX II Local Console also provides access to:

- Factory Reset
- Local Port Settings

Note: Only users with administrative privileges can access these functions.

KSX II Local Console Local Port Settings

From the Local Port Settings page, you can customize many settings for the KSX II Local Console including keyboard, local port hot key, video switching delay, power save mode, local user interface resolution settings, and local user authentication.

Note: This feature is available only on the KSX II Local Console.

► **To configure the local port settings:**

1. Choose Device Settings > Local Port Settings. The Local Port Settings page opens.
2. Choose the appropriate keyboard type from among the options in the drop-down list:
 - US
 - US/International
 - United Kingdom
 - French (France)
 - German (Germany)
 - JIS (Japanese Industry Standard)
 - Simplified Chinese
 - Traditional Chinese
 - Dubeolsik Hangul (Korean)

- German (Switzerland)
- Norwegian (Norway)
- Swedish (Sweden)
- Danish (Denmark)
- Belgian (Belgium)

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

3. Choose the local port hotkey. The local port hotkey is used to return to the KSX II 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

4. Set the Video Switching Delay from between 0 - 5 seconds, if necessary. Generally 0 is used unless more time is needed (certain monitors require more time to switch the video).
5. 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.
6. Choose the resolution for the KSX II Local Console from the drop-down list:
 - 800x600
 - 1024x768
 - 1280x1024
7. Choose the refresh rate from the drop-down list:
 - 60 Hz
 - 75 Hz
8. Choose the type of local user authentication:

- Local/LDAP/RADIUS. This is the recommended option. For more information about authentication, see Remote Authentication.
 - None. There is no authentication for Local Console access. This option is recommended for secure environments only.
9. Select the "Ignore CC managed mode on local port" checkbox if you would like local user access to the KSX II even when the device is under CC-SG management.

Note: If you initially choose not to ignore CC Manage mode on the local port but later want local port access, you will have to remove the device from under CC-SG management (from within CC-SG). You will then be able to check this checkbox.

10. Click OK.

► **To reset back to defaults:**

- Click Reset to Defaults.

KSX II Local Console Factory Reset

Note: This feature is available only on the KSX II Local Console.

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 212).*

► **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 device 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 device back to the default values (click Device Settings > Network Settings to access this information):
 - IP auto configuration
 - IP address
 - Subnet mask
 - Gateway IP address
 - Primary DNS server IP address
 - Secondary DNS server IP address
 - Discovery port
 - Bandwidth limit
 - LAN interface speed & duplex
 - Enable automatic failover
 - Ping interval (seconds)
 - Timeout (seconds)
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, the KSX II device is automatically restarted.

Resetting the KSX II Using the Reset Button

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** (on page 199)

*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 on the audit log. For more information about saving the audit log, see **Audit Log** (on page 212).*

► **To reset the device:**

1. Power off the KSX II.
2. Use a pointed object to press and hold the Reset button.
3. While continuing to hold the Reset button, power the KSX II device back on.
4. Continue holding the Reset button for 10 seconds.

Once the device has been reset, two short beeps signal its completion.



Chapter 14 Modem Configuration

In This Chapter

Certified Modems for UNIX, Linux and MPC	261
Low Bandwidth KVM Settings	262
Client Dial-Up Networking Configuration	263
Windows 2000 Dial-Up Networking Configuration	263
Windows Vista Dial-Up Networking Configuration	267
Windows XP Dial-Up Networking Configuration.....	268

Certified Modems for UNIX, Linux and MPC

Following is a list of modems that are certified to work for UNIX®, Linux®, and MPC:

- US Robotics Courier™ 56K Business Modem (Model# 3453B)
- Zoom/Fax Modem 56Kx Dualmode (Model# 2949)
- Zoom 56k v.92/v.90 Modem (Model # 3049)
- US Robotics v.92 56k Fax Modem (Model# 5686)
- US Robotics 56k SportSter® Modem

Low Bandwidth KVM Settings

Following are the settings that Raritan recommends in order to achieve optimum performance when using KVM over low bandwidth speeds typical of DSL connections. This information applies to both virtual KVM and MPC.

Setting	To achieve optimum performance:
Connection speed	Select Connections > Properties. Set the Connection Speed to a value that best matches the client-to-server connection. This ranges from 384 Kb (for lower DSL speeds) to >1MB.
Color depth	Select Connections > Properties. Reduce the Color Depth as far as possible. The lower this is set, the better the video refresh response on the target will be. The impact is noticeable when opening and moving folders on the target desktop. Specifically, the display is updated much quicker, improving the overall usability of the connection.
Noise filter	Select Video > Video Settings. The Noise Filter should be set to 7 (the highest value). At this setting, less bandwidth will be used for target screen changes, resulting in improved local and remote mouse synchronization.
<i>Note: Setting the color depth to low and the noise filter to high will cause a degradation in how the video is displayed. However, this tradeoff is offset by the overall improved usability due to better mouse synchronization and video update.</i>	
Smoothing	Select Connections > Properties. Set Smoothing to high. This will improve the appearance of target video by reducing the video noise that is displayed.
Auto color calibration	Select Video > Auto-sense Video Settings Deselect the Automatic Color Calibration checkbox to disable the option.
Quick sense video mode	Select Video > Video Settings to open the Settings dialog.

Setting	To achieve optimum performance:
	Select the "Quick sense video mode" radio to enable this option.

Client Dial-Up Networking Configuration

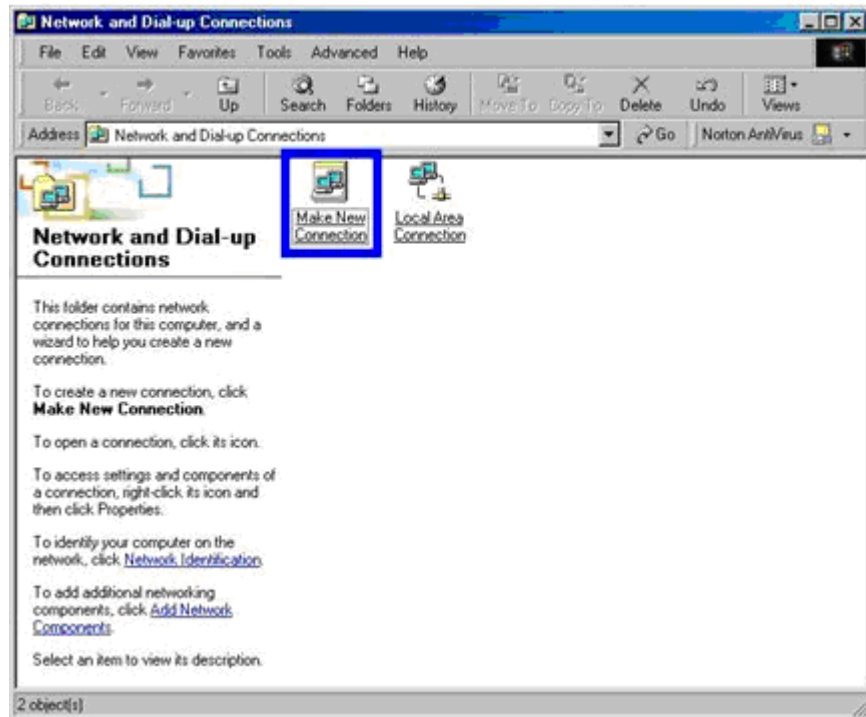
Configuring Microsoft Windows® Dial-Up Networking for use with KSX II allows configuration of a PC to reside on the same PPP network as the KSX II. After the dial-up connection is established, connecting to a KSX II is achieved by pointing the web browser to the PPP Server IP. Modem installation guidelines are provided for the following client based systems:

- Windows 7®
- Windows XP® operating system
- Windows Vista®

Windows 2000 Dial-Up Networking Configuration

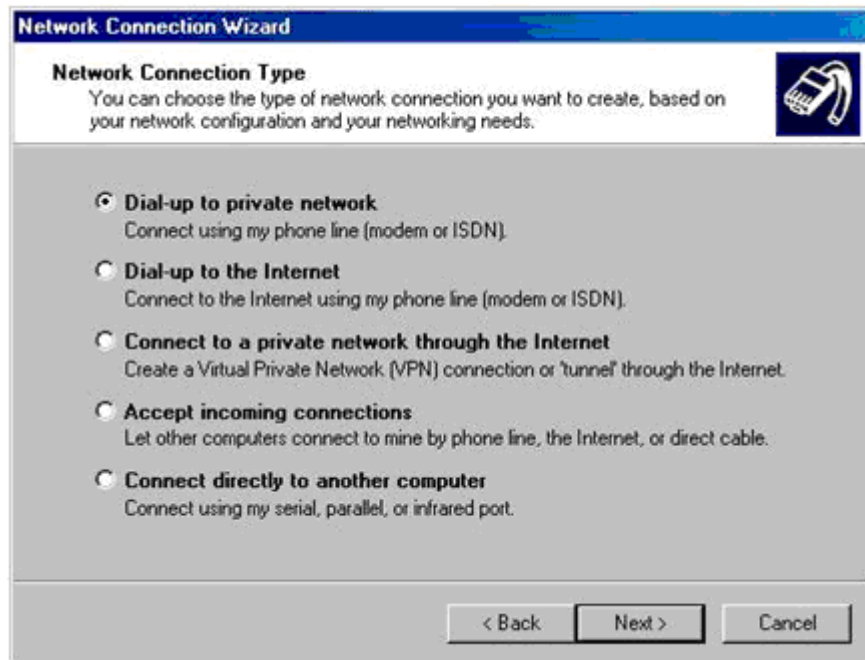
1. Choose Start > Programs > Accessories > Communications > Network and Dial-Up Connections.

2. Double-click the Make New Connection icon when the Network and Dial-Up Connections window appears.

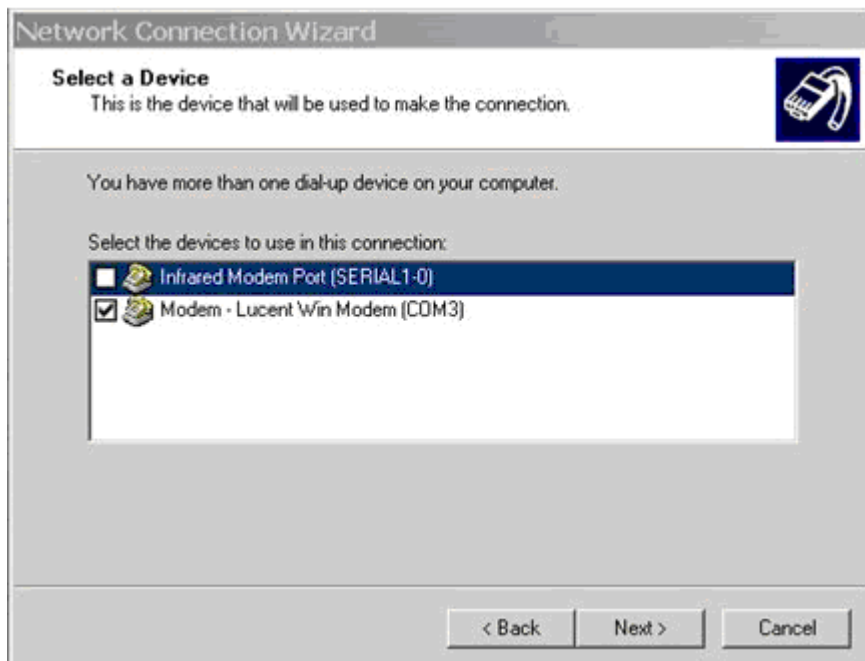


3. Click Next and follow the steps in the Network Connection Wizard dialog to create custom dial-up network profiles.

4. Click the Dial-up to private network radio button and click Next.

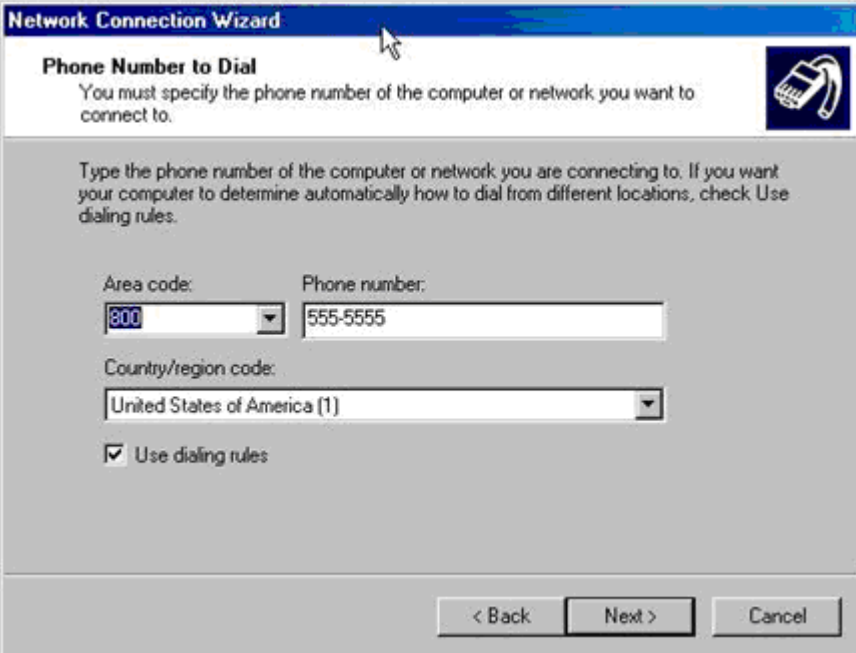


5. Select the checkbox before the modem that you want to use to connect to the KSX II and then click Next.



6. Type the area code and phone number you wish to dial in the appropriate fields.

- Click the Country/region code drop-down arrow and select the country or region from the list.



The screenshot shows the 'Network Connection Wizard' dialog box, specifically the 'Phone Number to Dial' step. The title bar reads 'Network Connection Wizard'. Below the title bar, the section is titled 'Phone Number to Dial' with a sub-instruction: 'You must specify the phone number of the computer or network you want to connect to.' To the right of the text is a small icon of a modem. The main area contains instructions: 'Type the phone number of the computer or network you are connecting to. If you want your computer to determine automatically how to dial from different locations, check Use dialing rules.' Below this, there are two input fields: 'Area code:' with a dropdown menu showing '800' and 'Phone number:' with a text box containing '555-5555'. Below these is a 'Country/region code:' dropdown menu showing 'United States of America (1)'. At the bottom left, there is a checked checkbox labeled 'Use dialing rules'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- Click Next. The Connection Availability dialog appears.
- Click the Only for myself radio button in the Connection Availability dialog.



The screenshot shows the 'Network Connection Wizard' dialog box, specifically the 'Connection Availability' step. The title bar reads 'Network Connection Wizard'. Below the title bar, the section is titled 'Connection Availability' with a sub-instruction: 'You may make the new connection available to all users, or just yourself.' To the right of the text is a small icon of a modem. The main area contains instructions: 'You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.' Below this, there is a section titled 'Create this connection:' with two radio buttons: 'For all users' (which is selected) and 'Only for myself'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

10. Click Next. The Network Connection has been created.
11. Type the name of the Dial-up connection.
12. Click Finish.
13. Click Dial to connect to the remote machine when the Dial dialog appears. A dialog indicating that a successful connection has been established will appear.

Consult the Windows 2000® Dial-up Networking Help if you receive any error messages.

Windows Vista Dial-Up Networking Configuration

1. Click Start and then click Network. The Network window opens.
2. Select Network and Sharing Center at the top of the window. The Network and Sharing Center window opens.
3. Select "Set up a Connection or Network".
4. Select "Set up a dial-up connection". The "Set up a dial-up connection" dialog appears.
5. Enter the dial-up number.
6. Enter your username and password.

Note: In order to access the KSX II, the username and password cannot use a \ (backslash).

7. Click Connect.

Set up a dial-up connection

Type the information from your Internet service provider (ISP)

Dial-up phone number: [Dialing Rules](#)

User name:

Password: ☐ Show characters ☒ Remember this password

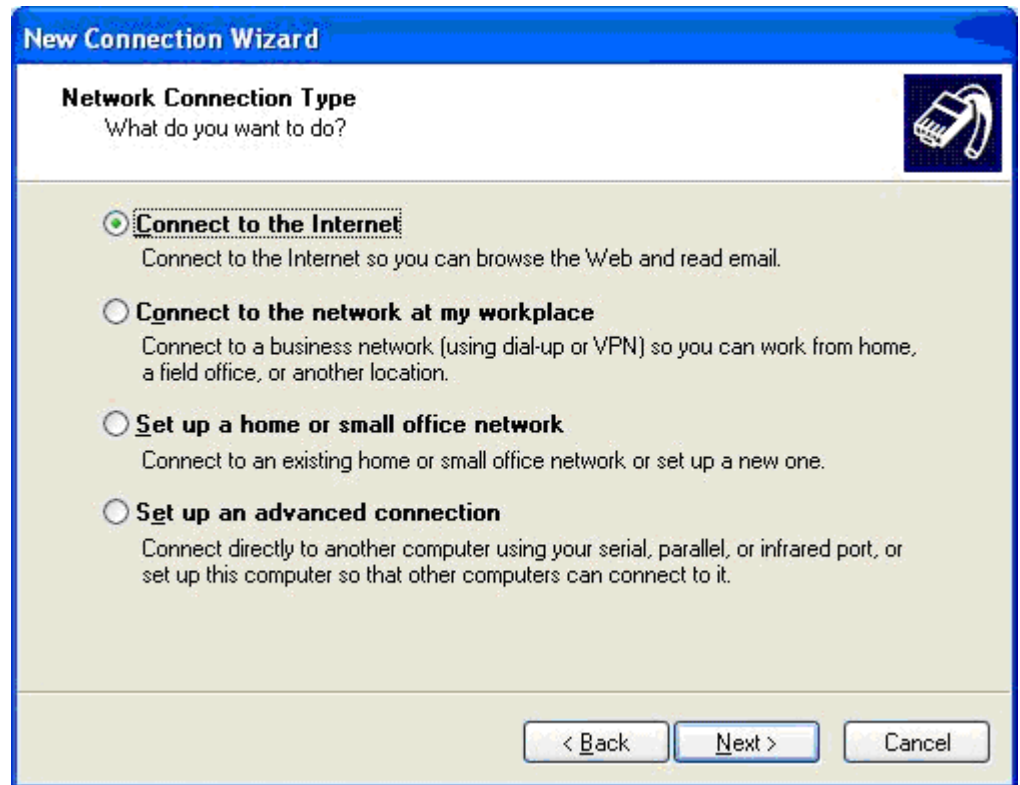
Connection name:

☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

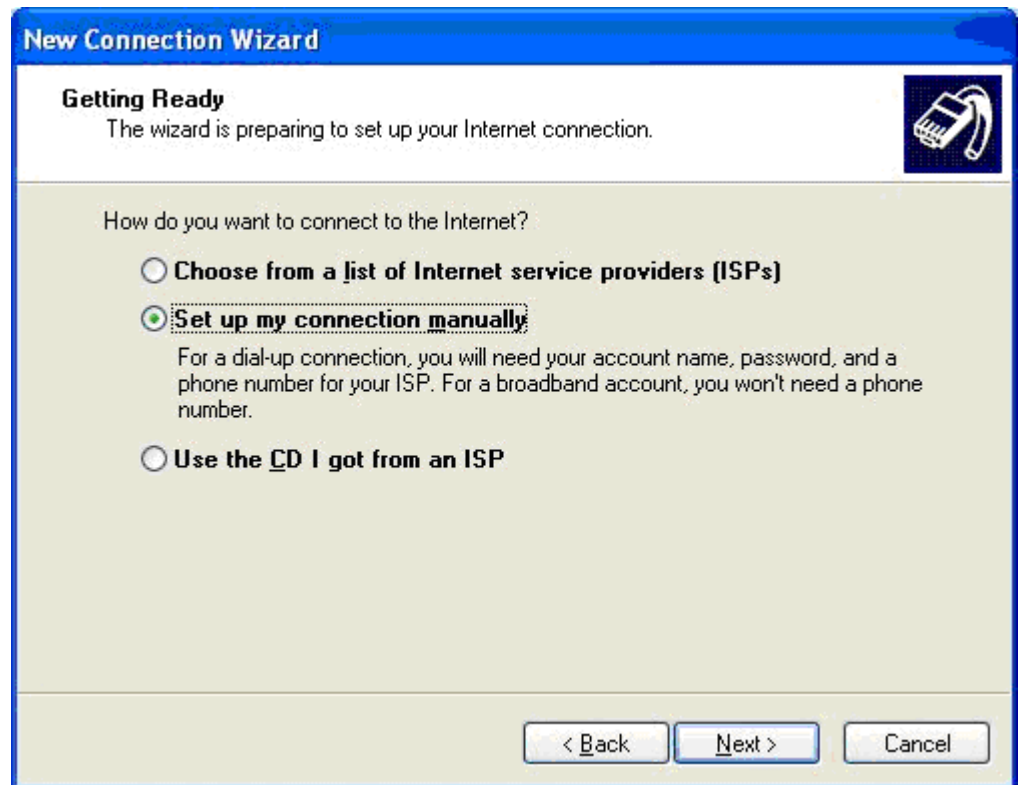
[I don't have an ISP](#)

Windows XP Dial-Up Networking Configuration

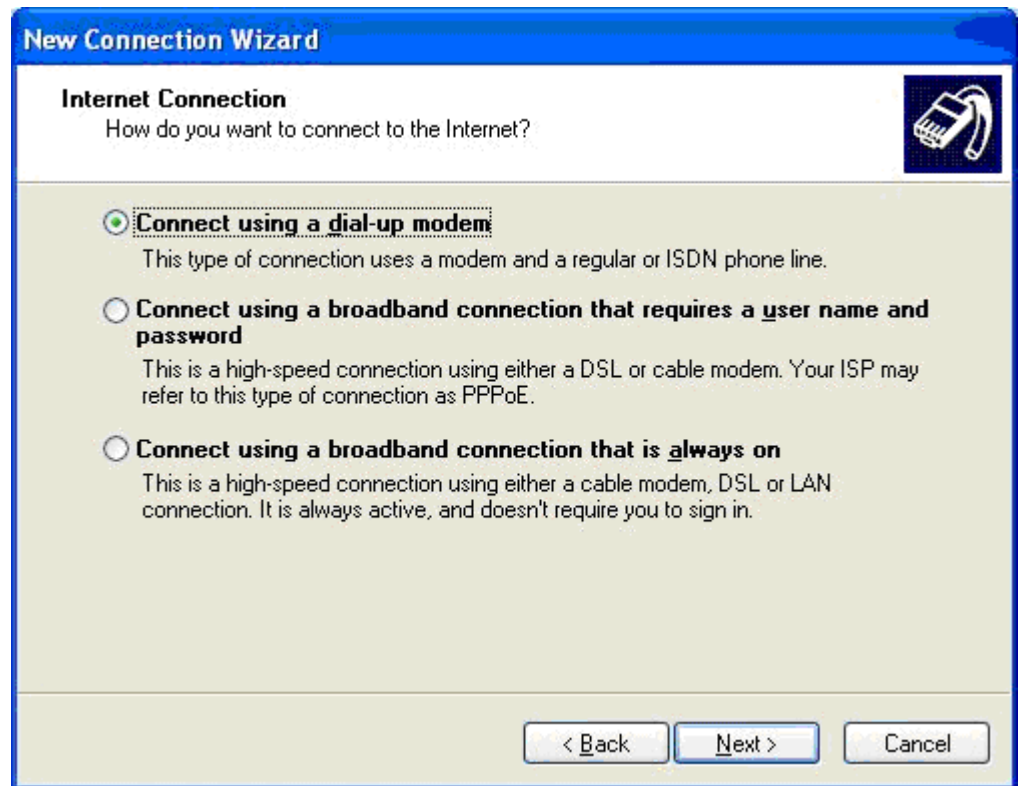
1. Choose Start > Programs > Accessories > Communications > New Connection Wizard.
2. Click Next and follow the steps in the New Connection Wizard to create custom dial-up network profiles.
3. Click the Connect to the Internet radio button and click Next.



- Click the "Set up my connection manually" radio button and click Next.



5. Click the "Connect using a dial-up modem" radio button and click Next.



6. Type a name to identify this particular connection in the ISP Name field and click Next.



The image shows a Windows-style dialog box titled "New Connection Wizard". It has a blue title bar and a light beige main area. In the top right corner of the main area, there is a small icon of a modem. The text "Connection Name" is displayed in bold. Below it, a question asks for the name of the service that provides the Internet connection. A instruction tells the user to type the name of their ISP in the following box. Below this is a text input field labeled "ISP Name" which contains the text "DominionKSX". A note states that the name typed here will be the name of the connection being created. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

New Connection Wizard

Connection Name
What is the name of the service that provides your Internet connection?

Type the name of your ISP in the following box.

ISP Name

DominionKSX

The name you type here will be the name of the connection you are creating.

< Back Next > Cancel

7. Type the phone number for the connection in the Phone number field and click Next.



The image shows a Windows-style dialog box titled "New Connection Wizard". The main heading is "Phone Number to Dial" with a sub-question "What is your ISP's phone number?". On the right is a small icon of a modem. The instruction "Type the phone number below." is followed by a text input field labeled "Phone number:" containing the text "8888888888". Below the field is a paragraph of help text: "You might need to include a '1' or the area code, or both. If you are not sure you need the extra numbers, dial the phone number on your telephone. If you hear a modem sound, the number dialed is correct." At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

New Connection Wizard

Phone Number to Dial
What is your ISP's phone number?

Type the phone number below.


Phone number:
8888888888

You might need to include a "1" or the area code, or both. If you are not sure you need the extra numbers, dial the phone number on your telephone. If you hear a modem sound, the number dialed is correct.

< Back Next > Cancel

8. Type your ISP information. Type the user name and password in the appropriate fields, and retype the password to confirm it.

9. Select the checkbox before the appropriate option below the fields and click Next.



The screenshot shows a Windows XP-style dialog box titled "New Connection Wizard". The main heading is "Internet Account Information". Below the heading, a message states: "You will need an account name and password to sign in to your Internet account." To the right of this message is a small icon of a modem. Below the message, instructions read: "Type an ISP account name and password, then write down this information and store it in a safe place. (If you have forgotten an existing account name or password, contact your ISP.)". There are three input fields: "User name:" with the text "admin", "Password:" with masked characters "••••••••", and "Confirm password:" with masked characters "••••••••". Below these fields are two checkboxes: the first is "Use this account name and password when anyone connects to the Internet from this computer" (unchecked), and the second is "Make this the default Internet connection" (unchecked). At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

10. Click Finish.
11. Click Dial to connect to the remote machine when the Dial dialog appears. A dialog indicating that you connected successfully appears. If you get any errors, consult Windows XP® Dial-up Networking Help.

Note: The maximum modem speed connecting to the KSX II is 33,600 bps, as it is a Linux® default limitation.

Appendix A Specifications

In This Chapter

Hardware	274
Software.....	297

Hardware

KSX II Dimensions and Physical Specifications

Line item description	UPC code	Power	Weight	Product dimensions (WxDxH)	Shipping weight	Shipping dimensions (WxDxH)
4 KVM and 4 Serial Port KSX II with multiple user network access and local port; virtual media.	785813650054	100/240 V 50/60 Hz 0.6A 27 Watts	8.65 lbs	1.75" x 17.3" x 11.4"	14.85 lbs	22" x 16.6" x 6.5"
			3.9kg	44mm x 439mm x 290mm	6.7 kg	559mm x 422mm x 165mm
KSX21888 KVM and 8 Serial Port KSX II with multiple user network access and local port; virtual media.	785813650047	100/240 V 50/60 Hz 0.6A 27 Watts	8.65 lbs	1.75" x 17.3" x 11.4"	14.85 lbs	22" x 16.6" x 6.5"
			3.9kg	44mm x 439mm x 290mm	6.7 kg	559mm x 422mm x 165mm

KSX II Environmental Requirements - KSX II

Operating	
Temperature	0°C- 40°C (32°F - 104°F)
Humidity	20% - 85% RH
Altitude	N/A
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A
Non-Operating	
Temperature	0°C- 50°C (32°F - 122°F)

Operating	
Humidity	10% - 90% RH
Altitude	N/A
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A

KSX II Electrical Specifications

Parameter	Value
Input	
Nominal Frequencies	50/60 Hz
Nominal Voltage Range	100/240 VAC
Maximum Current AC RMS	0.6A max.
AC Operating Range	100 to 240 VAC (+-10%), 47 to 63 Hz

KVM Properties

- Keyboard - USB
- Mouse - USB
- Video - VGA

Supported Target Server Video Resolution/Refresh Rate/Connection Distance

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:

Video resolution	Refresh rate	Maximum distance
1920x1080	60	50 ft. (15 m)
1600x1200	60	50 ft. (15 m)
1280x1024	60	100 ft. (30 m)
1024x768	60	150 ft. (45 m)




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.

See **Supported Video Resolutions** (on page 299) for the video resolutions supported by the KSX II.

Supported Computer Interface Module (CIMs) Specifications

CIM model	Description	Dimensions (WxDxH)	Weight
D2CIM-DVUSB	Dual USB CIM for BIOS virtual media, smartcard/CAC, audio and Absolute Mouse Synchronization 	1.7" x 3.5" x 0.8"; 43 x 90 x 19mm	0.25lb; 0.11kg
D2CIM-VUSB	USB CIM for virtual media and Absolute Mouse Synchronization 	1.3" x 3.0" x 0.6"; 33 x 76 x 15mm	0.20lb; 0.09kg
DCIM-PS2	CIM for PS/2	1.3" x 3.0" x 0.6"; 33 x 76 x 15mm	0.20lb; 0.09kg

CIM model	Description	Dimensions (WxDxH)	Weight
			
DCIM-SUN	CIM for Sun 	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
P2CIM-SER	Paragon II/Dominion KSX II CIM for serial (ASCII) devices 	1.3" x 3.0" x 0.6"; 33 x 76 x 15mm	0.20lb; 0.09kg

CIM model	Description	Dimensions (WxDxH)	Weight
D2CIM-DVUS B-DVI	Digital CIM that provides digital-to-analog conversion and support for 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-DVUS B-DP	Digital CIM that provides digital-to-analog conversion and support for 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-DVUS B-HDMI	Digital CIM that provides digital-to-analog conversion and support for 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

Digital CIM Target Server Timing and Video Resolution

Digital CIMs support Display Data Channels (DDC) and Enhanced Extended Display Identification Data (E-EDID).

See Supported Computer Interface Module (CIMs) Specifications for CIM specifications.

Digital CIM Timing Modes

Following are the default timing modes that are used when the KSX II 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.

- 1920x1080@60Hz
- 1600x1200@60Hz
- 1280x1024@60Hz (default resolution applied to digital CIMs)
- 1440x900@60Hz
- 1024x768@60Hz

See **Configuring CIM Ports** (on page 132) 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 KSX II 2.5.0 (and later).

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

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

Digital CIM Display Native Resolution

You are able to select the native resolution of the CIM on the Port Configuration page 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.

See **Configuring CIM Ports** (on page 132)

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 132) in online help.

Digital Video CIMs for Macs

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 KSX II 2.5.0 (and later) for Mac, see **Digital CIM Established and Standard Modes** (on page 280).

Supported Paragon II CIMS and Configurations

The KSX II 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	<ul style="list-style-type: none"> Servers with IBM® PS/2-type keyboard and mouse ports Automatic skew compensation (when the CIMS are connected to Paragon II, not from a KSX II) Intelligent Mouse mode Standard Mouse mode 	<ul style="list-style-type: none"> Virtual media Smart cards Absolute Mouse mode Use with blade chassis Cascaded KVM configurations
P2CIM-AUSBDUAL	<ul style="list-style-type: none"> 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 KSX II) Intelligent Mouse mode Standard Mouse mode 	<ul style="list-style-type: none"> Virtual media Smart cards Absolute Mouse mode Use with blade chassis Cascaded KVM configurations

KSX II-to-KSX II Paragon CIM Guidelines

The following system configuration guidelines should be followed when you are using Paragon CIMs in a KSX II-to-KSX II configuration:

Concurrent Access

Both KSX II 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 KSX II 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 KSX II. User Group PC Share permissions must not be relied on if Privacy must be guaranteed when using the P2CIM-APS2DUAL or P2CIM-AUSBDUAL with the KSX II.

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 KSX II naming convention (32 characters).

When first connected to a KSX II, the Paragon name will be retrieved from memory and written into the CIM memory location used by KSX II. Subsequent queries for the CIM name or updates to the CIM name from the KSX II will be made to the memory location used by the KSX II. Updates will not be made by the KSX II to the memory location used by Paragon II.

When the CIM name is updated by one KSX II, the other KSX II 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 KSX II.

Port Status and Availability

The port status, displayed on the KSX II Port Access page as either Up or Down, is updated to show whether the CIM is powered up and connected to the KSX II port.

The port availability, as displayed on the KSX II Port Access page as Idle, Busy or Connected, is only updated to reflect activity on a target that has been initiated from that same KSX II.

If a connection to the target is in place from the other KSX II, the availability is checked when a connection is attempted. Access is denied or allowed consistent with the PC-Share policy in place for the KSX II. Until that time, the availability is not be updated on the other KSX II.

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 KSX II. When the target is connected to two managed KSX IIs 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 KSX II.

If the KSX IIs 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 KSX II. The corresponding port name of the other KSX II will not be updated in CC-SG until a connection is attempted to the target port via the other KSX II's oob-kvm interface.

KSX II-to-Paragon II Guidelines

The P2CIM-APS2DUAL or P2CIM-AUSBDUAL can be connected to a KSX II and Paragon II.

Concurrent Access

The KSX II 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 KSX II must be set to Private. The Private setting is applied on to KSX II 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 KSX II. 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 KSX II are stored and retrieved from the CIM memory location corresponding to the KSX II naming convention.
- CIM name updates do not propagate between the Paragon II and the KSX II.

Supported Remote Connections

Remote connection	Details
Network	10BASE-T, 100BASE-T, and 1000BASE-T (Gigabit) Ethernet
Protocols	TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

Network Speed Settings

KSX II network speed setting

Network switch port setting	Auto	1000/Full	100/Full	100/Half	10/Full	10/Half
Auto	Highest Available Speed	1000/Full	KSX II: 100/Full Switch: 100/Half	100/Half	KSX II: 10/Full Switch: 10/Half	10/Half
1000/Full	1000/Full	1000/Full	No Communication	No Communication	No Communication	No Communication
100/Full	KSX II: 100/Half Switch: 100/Full	KSX II: 100/Half Switch: 100/Full	100/Full	KSX II: 100/Half Switch: 100/Full	No Communication	No Communication
100/Half	100/Half	100/Half	KSX II: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
10/Full	KSX II: 10/Half Switch: 10/Full	No Communication	No Communication	No Communication	10/Full	KSX II: 10/Half Switch: 10/Full
10/Half	10/Half	No Communication	No Communication	No Communication	KSX II: 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 KSX II behavior deviates from expected behavior

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

Supported Distances for Serial Devices

Following are the standard distances for serial devices:

Baud rate-feet
9600 - 100 ft.
28800 - 25 ft.
19200 - 50 ft.
38400 - 25 ft.
57600 - 16 ft.
115200 - 8 ft.

Connectivity

The following table lists the necessary KSX II hardware (adapters and/or cables) for connecting the KSX II to common vendor/model combinations.

Vendor	Device	Console connector	Serial connection
Checkpoint	Firewall	DB9M	ASCADB9F adapter and a CAT 5 cable
Cisco	PIX Firewall		
Cisco	Catalyst	RJ-45	CRLVR-15 rollover cable; or CRLVR-1 adapter cable and a CAT5 cable CRLVR-1 cable

Vendor	Device	Console connector	Serial connection
			for connecting a terminal port (RJ-45 Connector type) of KSX II-48 models that have this connector to another KSX II.
Cisco	Router	DB25F	ASCSDDB25M adapter and a CAT 5 cable
Hewlett Packard®	UNIX® Server	DB9M	ASCSDDB9F adapter and a CAT 5 cable
Silicon Graphics	Origin		
Sun™	SPARCStation	DB25F	ASCSDDB25M adapter and a CAT 5 cable
Sun	Netra T1	RJ-45	CRLVR-15 cable; or CRLVR-1 adapter and a CAT5 cable
Sun	Cobalt	DB9M	ASCSDDB9F adapter and a CAT 5 cable
Various	Windows NT®		

Go to the Support page on Raritan's website (www.raritan.com) to obtain a list of commonly used cables and adapters.

Emergency Connectivity

Connection	Description
Optional modem connectivity	For emergency remote access if the network has failed
Target device connectivity	Simplified RJ45-based CAT 5 cable scheme; serial port adapters are available from Raritan
Local access	Local Access for “crash-cart” applications

See **Connectivity** (on page 287) for a list of necessary KSX II hardware (adapters and/or cables) for connecting the KSX II to common Vendor/Model combinations.

TCP and UDP Ports Used

Port	Description
HTTP, Port 80	<p>This port can be configured as needed. See HTTP and HTTPS Port Settings (on page 164).</p> <p>By default, all requests received by the KSX II via HTTP (port 80) are automatically forwarded to HTTPS for complete security.</p> <p>The KSX II responds to Port 80 for user convenience, relieving users from having to explicitly type in the URL field to access the KSX II, while still preserving complete security.</p>
HTTPS, Port 443	<p>This port can be configured as needed. See HTTP and HTTPS Port Settings (on page 164).</p> <p>By default, this port is used for multiple purposes, including the web server for the HTML client, the download of client software (Multi-Platform Client (MPC) and Virtual KVM Client (VKC)) onto the client's host, and the transfer of KVM and virtual media data streams to the client.</p>
KSX II (Raritan KVM-over-IP) Protocol, Configurable Port 5000	<p>This port is used to discover other Dominion devices and for communication between Raritan devices and systems, including CC-SG for devices that CC-SG management is available.</p> <p>By default, this is set to Port 5000, but you may configure it to use any TCP port not currently in use. For details on how to configure this setting, see Network Settings (on page 124).</p>
SNTP (Time Server) on Configurable UDP Port 123	<p>The KSX II offers the optional capability to synchronize its internal clock to a central time server.</p> <p>This function requires the use of UDP Port 123 (the standard for SNTP), but can also be configured to use any port of your designation. Optional</p>
LDAP/LDAPS on Configurable Ports 389 or 636	<p>If the KSX II is configured to remotely authenticate user logins via the LDAP/LDAPS protocol, ports 389 or 636 will be used, but the system can also be configured to use any port of your designation. Optional</p>
RADIUS on Configurable Port 1812	<p>If the KSX II is configured to remotely authenticate user logins via the RADIUS protocol, either port 1812 will be used, but the system can also be configured to use any port of your designation. Optional</p>
RADIUS Accounting on Configurable Port 1813	<p>If the KSX II is configured to remotely authenticate user logins via the RADIUS protocol, and also employs RADIUS accounting for event logging, port 1813 or an additional port of your designation will be used to transfer log notifications.</p>
SYSLOG on Configurable UDP Port 514	<p>If the KSX II is configured to send messages to a Syslog server, then the indicated port(s) will be used for communication - uses UDP Port 514.</p>
SNMP Default UDP Ports	<p>Port 161 is used for inbound/outbound read/write SNMP access and port 162 is used for outbound traffic for SNMP traps. Optional</p>
TCP Port 22	<p>Port 22 is used for the KSX II command line interface (when you are</p>

Port	Description
	working with Raritan Technical Support).
SSH	(Secure Shell) SSH port can be configured. The default is port 22.
Telnet	Telnet port can be configured but is not recommended. The default port is 23.

Smart Card Minimum System Requirements

Local Port Requirements

The basic interoperability requirement for local port attachment to the KSX II 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 KSX II. If you are working with .NET 3.5 in a Windows XP environment on the target server, you must be using SP1.

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.

Linux Clients

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 and MPC, too.

Supported and Unsupported Smart Card Readers

External, USB smart card readers are supported.

Supported Smart Card Readers

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 CCID-compliant)
USB Token	Aladdin®	eToken PRO™	Proprietary implementation

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 KSX II 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	✓	✓	
Press D during startup	Start up in Apple Hardware Test (AHT)	✓ May need BIOS Mac profile for the mouse to work	✓ May need BIOS Mac profile for mouse to work	✓ 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		✓	✓
Press Option during startup	Start up in Startup Manager, where you	✓	✓	✓

Keystroke	Description	Virtual Media CIM	Dual Virtual Media CIM	Mac Lion Server HDMI CIM
	can select a Mac OS X volume to start from			
Press Eject, F12, or hold the mouse button	Ejects any removable media, such as an optical disc	✓	✓	
Press N during startup	Start up from a compatible network server (NetBoot)	✓	✓	✓
Press T during startup	Start up in Target Disk mode			✓
Press Shift during startup	Start up in Safe Boot mode and temporarily disable login items	✓	✓	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	✓	✓	✓
Press Command-S during startup	Start up in Single-User mode	✓	✓	✓
Press Option-N during startup	Start from a NetBoot server using the default boot image	✓	✓	✓
Press Command-R during startup	Start from Lion Recovery1	N/A	N/A	✓

Using a Windows Keyboard to Access Mac Targets

A Windows® keyboard can be used to access a Mac® connected to a KSX II. Windows keys are then used to emulate the special Mac keys. This is the same as connecting a Windows keyboard directly to the Mac.

KSX II Serial RJ-45 Pinouts

To provide maximum port density and to enable simple UTP (Category 5) cabling, The KSX II provides its serial connections via compact RJ-45 ports. However, no widely adopted industry-standard exists for sending serial data over RJ-45 connections.

The following tables list the RJ-45 pinouts for the RJ-45 connector.

RJ-45 PIN	SIGNAL
1	RTS
2	DTR
3	TxD
4	GND
5	DCD
6	RxD
7	DSR
8	CTS

Go to the Raritan website (www.raritan.com) Support page to find the latest information about the KSX II serial pinouts (RJ-45).

DB9F Nulling Serial Adapter Pinouts

RJ-45 (female)	DB9 (female)
1	8
2	1, 6
3	2
4	SHELL
5	5
6	3
7	4
8	7

DB9M Nulling Serial Adapter Pinouts

RJ-45 (female)	DB9 (male)
1	8
2	1, 6
3	2
4	SHELL
5	5
6	3
7	4

RJ-45 (female)	DB9 (male)
8	7

DB25F Nulling Serial Adapter Pinouts

RJ-45 (female)	DB25 (female)
1	5
2	6, 8
3	3
4	1
5	7
6	2
7	20
8	4

DB25M Nulling Serial Adapter Pinouts

RJ-45 (female)	DB25 (male)
1	5
2	6, 8
3	3
4	1
5	7
6	2
7	20
8	4

Software

Supported Operating Systems (Clients)

The following operating systems are supported on the Virtual KVM Client (VKC) and Multi-Platform Client (MPC).

- Windows 7®
- Windows XP®
- Windows 2008®
- Windows Vista®
- Windows 2000® SP4 Server
- Windows 2003® Server
- Windows 2008® Server
- Red Hat® Desktop 5.0
- Red Hat Desktop 4.0
- Open SUSE 10, 11
- Fedora® 13 and 14
- Mac® OS X
 - Mac® OS X Mountain Lion® 10.7.5 using Safari 6.0.5 running JRE™ 1.7.0_51
 - Mac OS X Mountain Lion 10.8.5 * using Safari 6.1.1 running JRE 1.7.0_51

**Note: Upon upgrading from OS X 10.8.2 to OS X 10.8.3, Safari® may block Java™.*

- Solaris™

Note: Solaris does not support virtual media for ISO images.

- Linux®

The JRE™ plug-in is available for the Windows® 32-bit and 64-bit operating systems. MPC and VKC can be launched only 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®	<ul style="list-style-type: none"> • Internet Explorer® 6.0 SP1+ or 7.0, 9.0, 10.0 or 11.0 • Firefox® 1.06 - 4 or later
	Windows Server 2003®	<ul style="list-style-type: none"> • Internet Explorer 6.0 SP1++, 9.0, 10.0 or 11.0 • Firefox 1.06 - 3
	Windows Vista®	<ul style="list-style-type: none"> • Internet Explorer 9.0, 10.0 or 11.0
	Windows 7®	<ul style="list-style-type: none"> • 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:
	Windows XP Professional®	<ul style="list-style-type: none"> • Internet Explorer 6.0 SP1+, 7.0 or 8.0 • Firefox 1.06 - 4 or later
	Windows XP Tablet®	
	Windows Vista	64bit mode, 64bit browsers:
	Windows Server 2003	<ul style="list-style-type: none"> ▪ Internet Explorer 7.0, 8.0, 9.0, 10.0 or 11.0
	Windows Server 2008	
	Windows 7	

Supported Browsers

KSX II supports the following browsers:

- Internet Explorer® 7 through 11
- Firefox® 4 (or later)
- Safari® 3 (or later)
 - Mac® OS X Mountain Lion® 10.7.5 using Safari 6.0.5 running JRE™ 1.7.0_51

- Mac OS X Mountain Lion 10.8.5 * using Safari 6.1.1 running JRE 1.7.0_51

**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 7 (JRE)® on PCs and Macs® when using the Virtual KVM Client (VKC) to access target servers via KSX II.

This ensures in order to provide high performance, KVM-over-IP video processing when remotely accessing target servers/PCs/Macs.

The latest version of JRE for Mac can be downloaded from the Apple 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 KSX II.

Certain versions of Safari® block Java for security reasons. Since Java is required to use KSX II, 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.

Supported Video Resolutions

Ensure each target server's video resolution and refresh rate are supported by the KSX II, and that the signal is noninterlaced.

Video resolution and cable length are important factors in the ability to obtain mouse synchronization.

The KSX II supports these resolutions:

Resolutions	
640x350 @70Hz	1024x768@85
640x350 @85Hz	1024x768 @75Hz
640x400 @56Hz	1024x768 @90Hz
640x400 @84Hz	1024x768 @100Hz
640x400 @85Hz	1152x864 @60Hz
640x480 @60Hz	1152x864 @70Hz
640x480 @66.6Hz	1152x864 @75Hz

Resolutions	
640x480 @72Hz	1152x864 @85Hz
640x480 @75Hz	1152x870 @75.1Hz
640x480 @85Hz	1152x900 @66Hz
720x400 @70Hz	1152x900 @76Hz
720x400 @84Hz	1280x720@60Hz
720x400 @85Hz	1280x960 @60Hz
800x600 @56Hz	1280x960 @85Hz
800x600 @60Hz	1280x1024 @60Hz
800x600 @70Hz	1280x1024 @75Hz
800x600 @72Hz	1280x1024 @85Hz
800x600 @75Hz	1360x768@60Hz
800x600 @85Hz	1366x768@60Hz
800x600 @90Hz	1368x768@60Hz
800x600 @100Hz	1400x1050@60Hz
832x624 @75.1Hz	1440x900@60Hz
1024x768 @60Hz	1600x1200 @60Hz
1024x768@70	1680x1050@60Hz
1024x768@72	1920x1080@60Hz

Note: Composite Sync and Sync-on-Green video require an additional adapter.

Note: Some resolutions may not be available by default. If you do not see a resolution, plug in the monitor first, remove the monitor and then plug in the CIM.

Note: If the 1440x900 and 1680x1050 resolutions are not displayed but are supported by the target server's graphics adapter card, a DDC-1440 or DDC-1680 adapter may be required.

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 132)

KSX II Supported Keyboard Languages

The KSX II 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 KSX II Local Console functions. For more information about non-US keyboards, see Informational Notes.

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 Traditional	Hong Kong S. A. R., Republic of China (Taiwan)	Chinese Traditional
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

Language	Regions	Keyboard layout
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

Appendix B Updating the LDAP/LDAPS Schema

IMPORTANT: The procedures in this chapter should be attempted only by experienced users.

In This Chapter

Returning User Group Information	303
Setting the Registry to Permit Write Operations to the Schema	304
Creating a New Attribute	304
Adding Attributes to the Class	305
Updating the Schema Cache.....	307
Editing rcusergroup Attributes for User Members	307

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 KSX II 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.

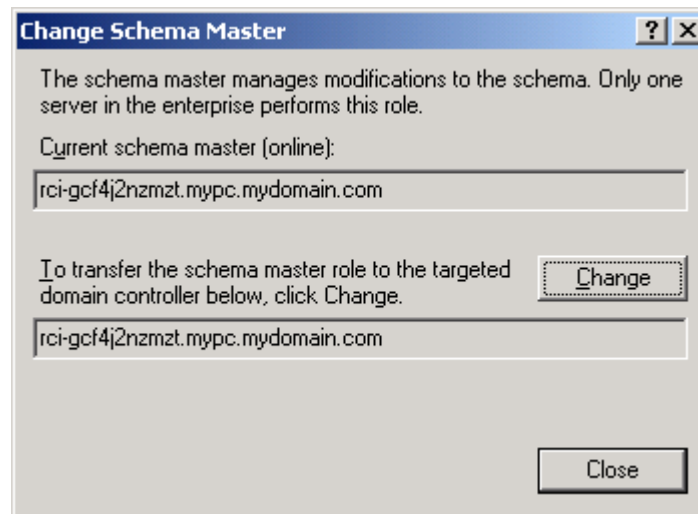
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

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.



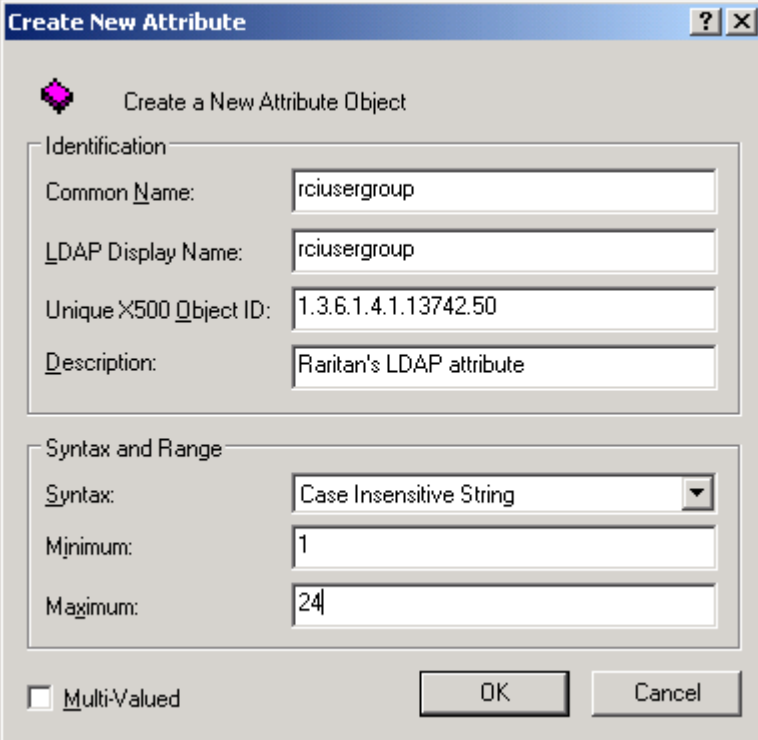
2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**
3. Click OK.

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 'Create New Attribute' dialog box with the following fields and values:

Create a New Attribute Object	
Identification	
Common Name:	rciusergroup
LDAP Display Name:	rciusergroup
Unique X500 Object ID:	1.3.6.1.4.1.13742.50
Description:	Raritan's LDAP attribute
Syntax and Range	
Syntax:	Case Insensitive String
Minimum:	1
Maximum:	24
<input type="checkbox"/> Multi-Valued <input type="button" value="OK"/> <input type="button" value="Cancel"/> 	

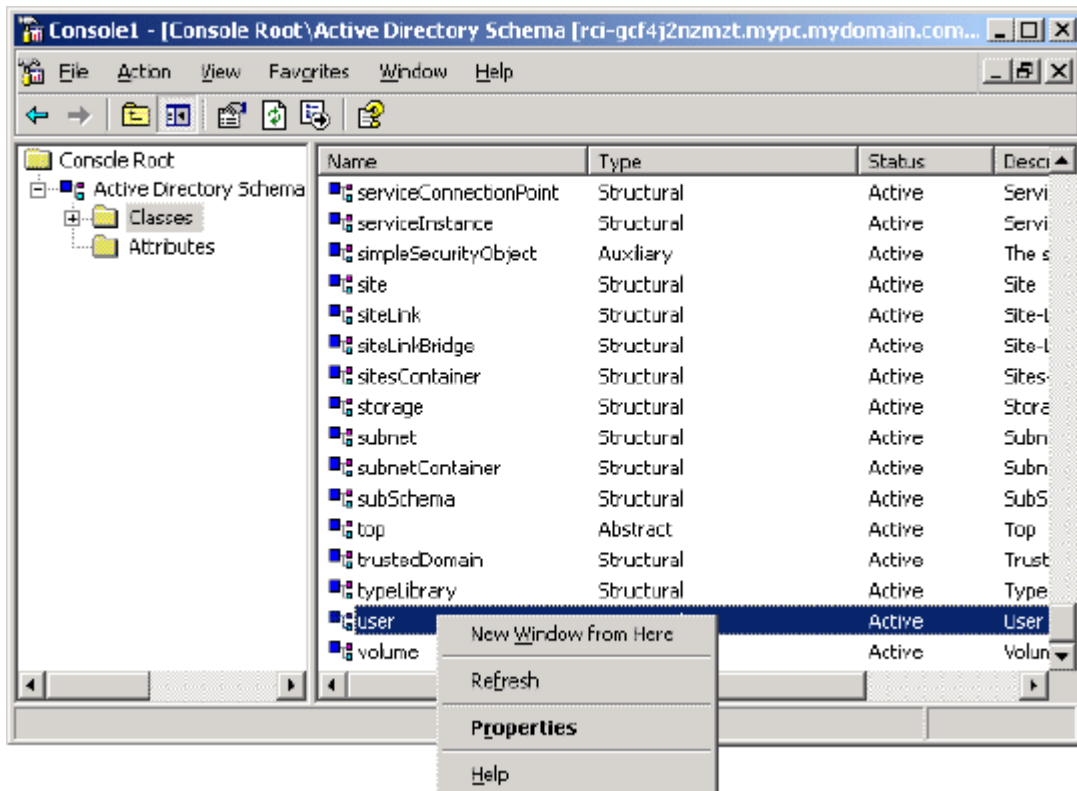
- Type *rciusergroup* in the Common Name field.
- Type *rciusergroup* in the LDAP Display Name field.
- Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
- Type a meaningful description in the Description field.
- Click the Syntax drop-down arrow and choose Case Insensitive String from 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:

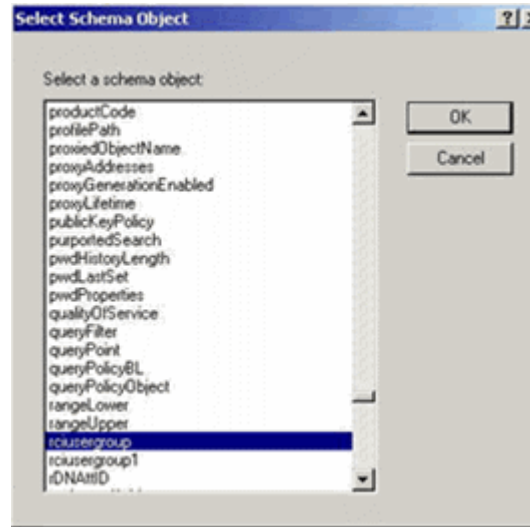
- Click Classes in the left pane of the window.

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.

6. Choose rcigroup from the Select Schema Object list.



7. Click OK in the Select Schema Object dialog.
8. Click OK in the User Properties dialog.

Updating the Schema Cache

► To update the schema cache:

1. Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.
2. Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

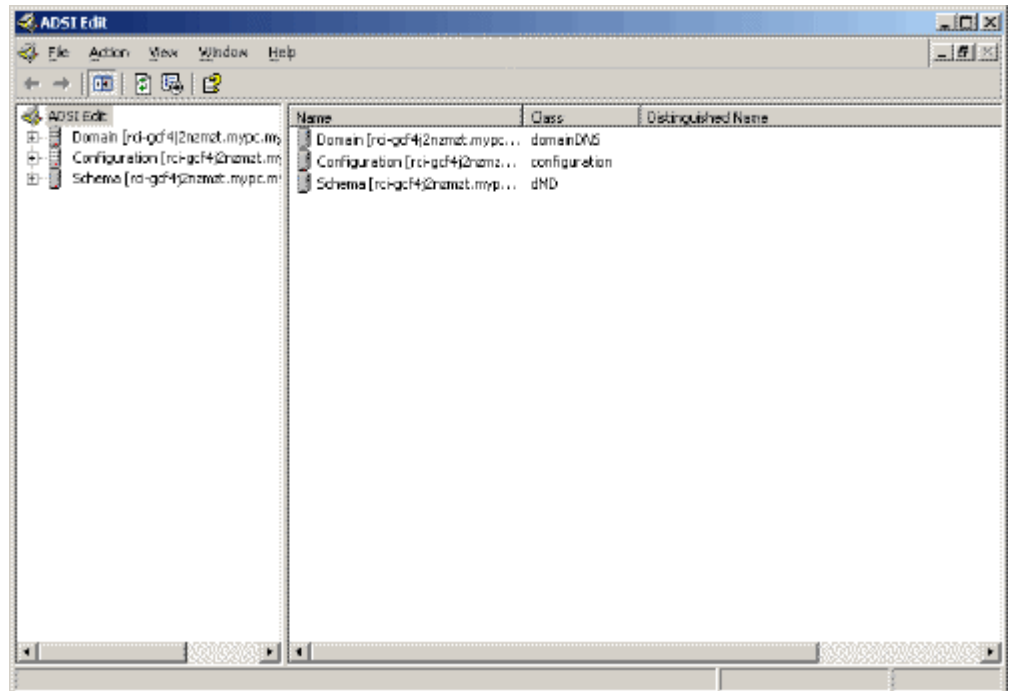
Editing rcigroup Attributes for User Members

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:

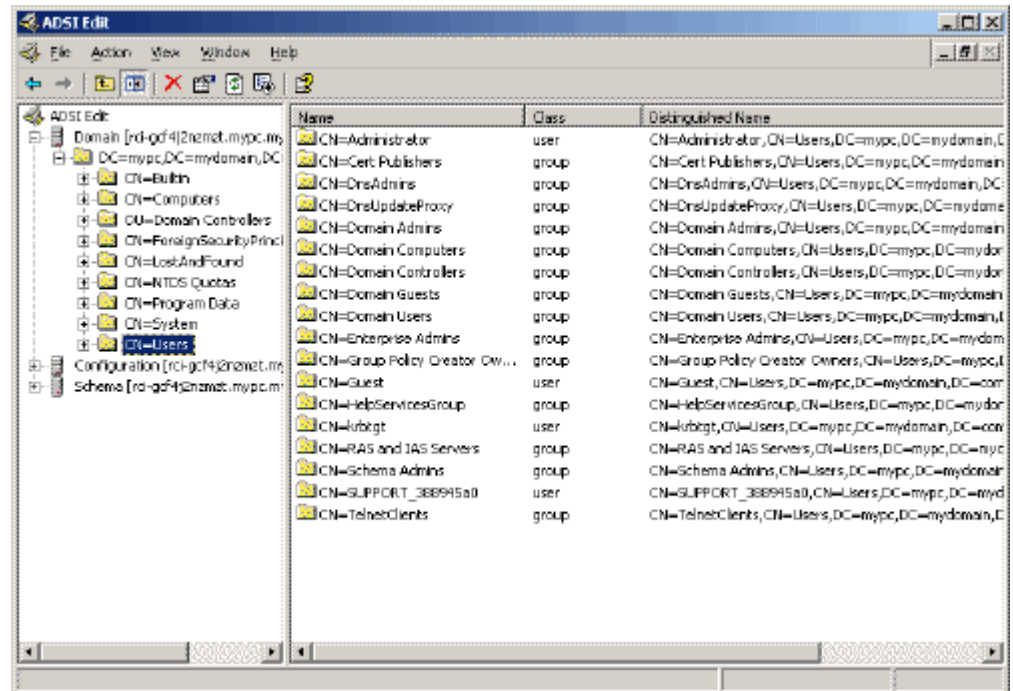
1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.

3. Go to the directory where the support tools were installed. Run `adsiedit.msc`. The ADSI Edit window opens.



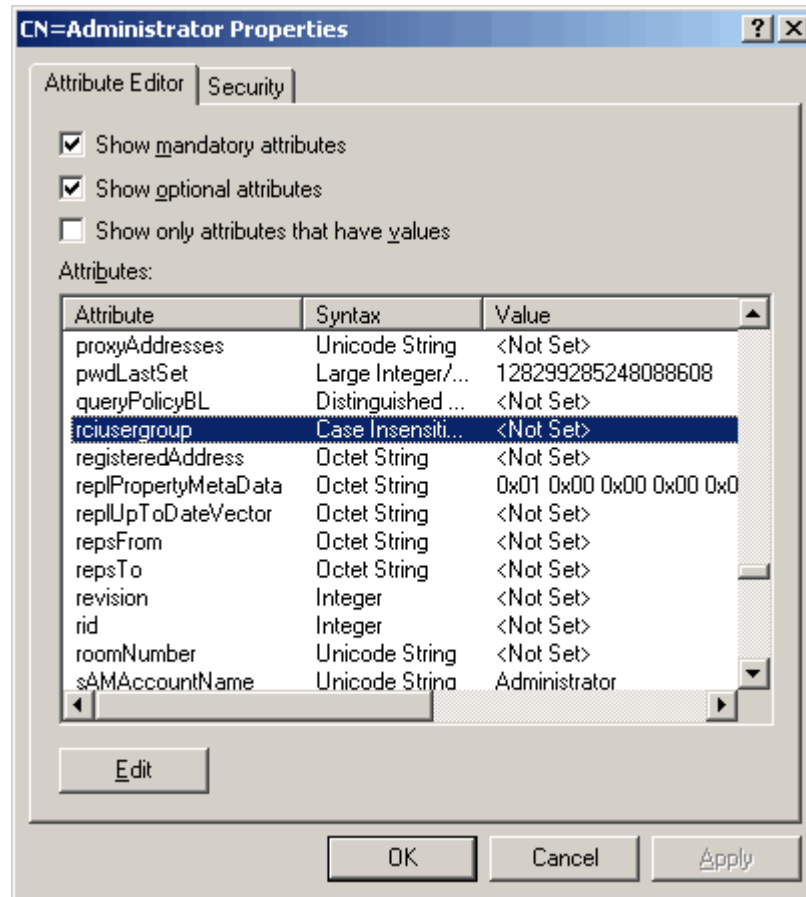
4. Open the Domain.

5. In the left pane of the window, select the CN=Users folder.

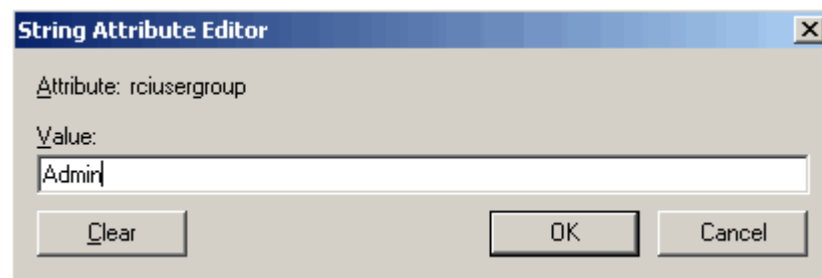


6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.

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 KSX II) in the Edit Attribute field. Click OK.



Appendix C Informational Notes

In This Chapter

Overview	311
Java Runtime Environment (JRE) Notes.....	311
IPv6 Support Notes	314
Dell Chassis Cable Lengths and Video Resolutions	315
CIM Notes.....	315
Virtual Media Notes	315
USB Port and Profile Notes	316
Keyboard Notes.....	319
CC-SG Notes.....	323
Browser Notes	323
VKC and MPC Smart Card Connections to Fedora Servers.....	324
SUSE/VESA Video Modes	324

Overview

This section includes important notes on KSX II usage. Future updates will be documented and available online through the Help link in the KSX II Remote Console interface.

Note: Some topics in this section reference other multiple Raritan devices because various devices are impacted by the information.

Java Runtime Environment (JRE) Notes

AES 256 Prerequisites and Supported Configurations for Java

Applications	Prerequisites	Supported
Standalone MPC	Requires installation of Java Cryptography Extension® (JCE®) Unlimited Strength Jurisdiction Policy Files +	Yes
Standalone RSC	Requires installation of Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files +	Yes

Applications	Prerequisites	Supported	
MPC Applet	Requires installation of Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files +	Browser	Supported
		Firefox® 2.0.0.7	Yes
		Firefox 3.0.x	Yes
		Internet Explorer® 6*	No
		Internet Explorer 7	Yes
		Internet Explorer 8	Yes
HTML access client	Requires installation of Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files +	Browser	Supported
		Firefox 2.0.0.7	Yes
		Firefox 3.0.x	Yes
		Internet Explorer 6 *	No
		Internet Explorer 7	Yes
		Internet Explorer 8	Yes

+ Jurisdiction files for various JREs™ are available in the Other Downloads on the Java™ Sun™ site.

JRE	Link
JRE1.6	http://java.sun.com/javase/downloads/index.jsp

* In addition, IE6 does not support AES 128.

Java Runtime Environment (JRE)

Important: It is recommended that you disable Java™ caching and clear the Java cache. Please refer to your Java documentation for more information.

The KSX II Remote Console and MPC require JRE™ to function. Java Runtime Environment™ (JRE) version 1.6.x or higher are supported. The KSX II Remote Console checks the Java version. If the version is incorrect or outdated, you will be prompted to download a compatible version.

Note: In order for multi-language keyboards to work in the KSX II Remote Console (Virtual KVM Client), install the multi-language version of Java Runtime Environment (JRE).

Java Not Loading Properly on Mac

If you are using a Mac® and see the following message when connecting to a device from the KSX II 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® and Windows 7 operating systems

The following IPv6 configurations *are not* supported by Java:

- J2SE does not support IPv6 on Microsoft® Windows®.

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 KSX II 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

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 KSX II:

Video resolution	Cable length
1024x768@60Hz	50' (15.24 m)
1280x1024@60Hz	50' (15.24 m)
1600x1200@60Hz	30' (9.14 m)

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.

Smart Card Reader Not Detected when Using a DVM-DP CIM

If you are using a DVM-DP CIM to connect to a target that has a smart card reader mounted on it, the smart card reader may not be detected. To resolve this issue, reinstall the smart card reader driver on the target.

Virtual Media Notes

Dell OptiPlex and Dimension Computers

From certain Dell OptiPlex™ and Dimension computers, it may not be possible to boot a target server from a redirected drive/ISO image, or to access the target server BIOS when a virtual media session is active (unless the Use Full Speed for Virtual Media CIM option is enabled from the Port page).

Note: ISO9660 format is the standard supported by Raritan. However, other CD-ROM extensions may also work.

Accessing Virtual Media on a Windows 2000

A virtual media local drive cannot be accessed on a Windows 2000® server using a D2CIM-VUSB.

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.

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

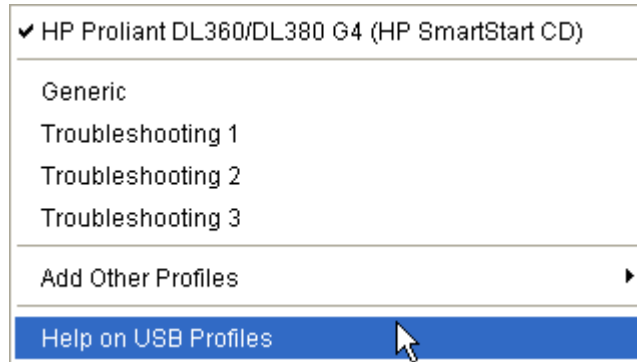
VM-CIMs and DL360 USB Ports

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** (on page 93).

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.

Keyboard Notes

Non-US Keyboards

French Keyboard

Caret Symbol (Linux® Clients Only)

The Virtual KVM Client (VKC) and the Multi-Platform Client (MPC) 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) and the Multi-Platform Client (MPC) , 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) and the Multi-Platform Client (MPC) , the numeric keypad symbols display as follows when using a French keyboard:

Numeric keypad symbol	Displays as
/	;
.	;

Tilde Symbol

From the Virtual KVM Client (VKC) and the Multi-Platform Client (MPC) , 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) and the Multi-Platform Client (MPC).

► **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.

Key Combinations and the Java Runtime Environment (JRE)

Because of a limitation in the Java Runtime Environment™ (JRE™), Fedora®, Linux®, and Solaris™ clients receive an invalid response from Alt Gr on UK English and US International language keyboards. Fedora, Linux, and Solaris do not pick up events for the Alt Gr key combination for Java™ 1.5. Java 1.6 appears to improve on this, although the keyPressed and keyReleased events for Alt Gr still identify it as an “unknown key code”.

Also, a key pressed in combination with Alt Gr (such as on the UK keyboard Alt Gr-4, which is the Euro symbol), only generates a keyTyped followed by a keyReleased event for that value without a keyPressed event. Java 1.6 improves upon this by filling in the keyPressed event as well.

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) and the Multi-Platform Client (MPC) are unable to process these keys from a Mac client's keyboard.

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”.

Single Mouse Mode when Connecting to a Target Under CC-SG Control

When using Firefox® to connect to a KSX II 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.

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 Fedora Core Focus

Using the Multi-Platform Client (MPC), occasionally there is an inability to log in to an LX, KX II or KSX II device, or to access KVM target servers (Windows®, SUSE, and so forth). In addition, the Ctrl+Alt+M key combination may not bring up the Keyboard Shortcut menu. This situation occurs with the following client configuration: Fedora® Core 6 and Firefox® 1.5 or 2.0.

Through testing, it has been determined that installation of libXp resolves window focusing issues with Fedora Core 6. Raritan has tested with libXp-1.0.0.8.i386.rpm; this resolved all of the keyboard focus and popup-menu problems.

Note: libXp is also required for the SeaMonkey (formerly Mozilla®) browser to work with the Java™ plug-in.

Mouse Pointer Synchronization (Fedora)

When connected in dual mouse mode to a target server 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).

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.

VKC and MPC Smart Card Connections to Fedora Servers

If you are using a smart card to connect to a Linux® Fedora® server via Multi-Platform Client (MPC) and Virtual KVM Client (VKC) upgrade the pcsc-lite library to 1.4.102-3 or above.

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 KSX II, 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 KSX II.

Appendix D KSX II FAQs

In This Chapter

FAQs.....325

FAQs

Question	Answer
What is the Dominion KSX II?	The Dominion KSX II is an integrated remote access and control appliance that provides secure, out-of-band KVM-over-IP, serial access and power control for IT assets in remote and branch offices.
What is the typical application of the KSX II?	The Dominion KSX II is targeted at centralized, remote management of IT devices at branch and remote offices. This enables IT administrators to remotely access, control and manage hundreds or even thousands of sites.
What types of IT equipment can the KSX II manage?	KSX II can manage KVM- and serially-controlled equipment, including computer servers and equipment, telecommunications gear and networking devices. KSX II can perform remote power control using the optional Dominion PX™ rack-based power distribution units (PDUs).
What types of remote management functions are supported?	<p>The KSX II provides complete, out-of-band, remote management. This includes BIOS level KVM-over-IP control, remote serial console access, remote power control and remote virtual media.</p> <p>KSX II provides complete remote management, regardless of the target device's state. You can enter at the BIOS level, run hardware diagnostics, reboot a hung server, install software from DVDs and even re-image a server.</p>
Can you describe a typical remote office customer?	The typical customer is a company with IT assets in multiple branch offices, looking for centralized remote management of those devices. Customers increasingly have dispersed IT assets, but do not have IT staff at these facilities. Examples of customers are: banks with multiple branches, retail chains with multiple stores and brokerage firms with multiple offices.

Question	Answer
Any other customer types?	<p>Another class of customer has multiple types of equipment in a rack, lab or office (or even a closet) and would like to manage these diverse devices remotely with a single secure appliance.</p> <p>By replacing two devices (KVM switch and serial console server) with a single appliance, customers will: (1) save money, (2) reduce rack space and cabling, (3) decrease energy usage and (4) increase productivity through anytime/anywhere remote access.</p>
What is the KSX II's value proposition?	<p>The KSX II's value proposition is based on anytime/anywhere, centralized, remote access and control of geographically dispersed equipment.</p> <p>KSX II customers benefit from: (1) reduced travel expenses,</p> <p>(2) increased IT productivity, (3) decreased mean time to repair and</p> <p>(4) higher service quality.</p>
Technical Features	
In a nutshell, what is the KSX II?	<p>The Dominion KSX II is a combination of the Dominion KX II KVM-over-IP switch and features from the Dominion SX Secure Console Server. It provides world-class KVM-over-IP, serial-over-IP and remote power control in a single appliance.</p>
What KSX II models are available?	<p>The Dominion KSX II is available in two secure hardware appliances.</p> <p>The DKSX-144 features four KVM-over-IP ports, four serial ports, two power control ports and a local port for direct access.</p> <p>The DKSX-188 features eight KVM-over-IP ports, eight serial ports, two power control ports and a local port for direct access.</p>

Question	Answer
How does the Dominion KSX II compare to the Dominion KX II?	<p>Built on a foundation of the award-winning Dominion KX II, the Dominion KSX II provides virtually all of the KX II's KVM-over-IP software features as of Release 2.5. As of KSX Release 2.5, servers with DVI, HDMI, and DisplayPort are supported via the new digital video CIMs. Note that the tiering (cascading) feature is one of the few exceptions. See the Dominion KX II Features and Benefits document for the complete KX II KVM-over-IP software features.</p> <p>In terms of hardware features, the KSX II has four or eight KVM-over-IP ports, four or eight dedicated serial ports, a single power supply, dual gigabit Ethernet LAN ports, local port, admin port, a built in modem and two dedicated power control ports.</p> <p>The KSX II supports a single KVM-over-IP remote connection, an independent local port KVM connection, and either four or eight serial port connections.</p>
How are remote power control strips connected to the KSX II?	<p>Dominion PX PDUs are connected via Cat5 cable to the two power ports on the KSX II. No CIMs are required.</p>
Does the KSX II have a modem port?	<p>Actually, the KSX II has a built in modem for emergency use if the primary network is down.</p>
What are some sample Dominion KX II features?	<p>Some sample Dominion KX II features available in the KSX II are:</p> <ul style="list-style-type: none"> Virtual media Absolute Mouse Synchronization™ Common HTML remote and local user interface Blade server support Mobile iPhone/iPad access Dual Stack IPv6/IPv4 FIPS 140-2 encryption module Smart card/CAC support 1080p HD remote video resolution <p>See the Dominion KX II Features and Benefits document for more information.</p>

Question	Answer
Is the Dominion KSX II FIPS 140-2-certified?	The Dominion KSX II uses a FIPS 140-2-certified encryption module for both serial and KVM sessions. The KSX II also supports DoD Common Access Card, Secure Login Banner and IPv6 -- three other features of interest to government and military customers.
How does the Dominion KSX II compare to the Dominion SX?	Like the Dominion SX, the KSX II supports true serial connections with dedicated serial ports and SX-like functionality. Select Dominion SX II features are supported by the KSX II including: True, remote serial access and control Access via Raritan Serial Client, SSH and Telnet Key logging and history Cut and paste Keyword monitoring and alerting Serial session disconnect commands Secure chat Direct port access
Is a CIM (dongle) required to access serial devices?	A CIM is not required for the KSX II as it provides a true serial connection – no serial converter or external power adapter is required. However, like the Dominion SX, an inexpensive serial adapter may be required based on the exact pin-out of the serial device.
What is virtual media?	Virtual media is a powerful feature that enables a user to mount drives and media from the user's desktop to remote servers during a KVM connection. This is ideal to install software, run hardware diagnostics, transfer files and even remotely reimage a server.
What types of virtual media does the Dominion KSX II support?	Dominion KSX II supports the following types of virtual media: internal and USB-connected CD/DVD drives, USB mass storage devices, PC hard drives and local and remote ISO images.
Is virtual media secure?	Yes. Virtual media sessions are secured using up to 256-bit AES or 128-bit RC4 encryption.

Question	Answer
Does the KSX II support the D2CIM-DVUSB?	Yes. With release 2.3, KSX II supports the dual USB virtual media CIM (and USB profile feature) which enable expanded BIOS use of virtual media drives to the broadest range of servers and BIOS versions.
What type of video is supported by your KVM CIMs?	Our CIMs have traditionally supported analog VGA video. Three new CIMs (see http://www.raritan.com/resources/application-briefs/digital-cim.pdf - http://www.raritan.com/resources/application-briefs/digital-cim.pdf) support digital video formats, including DVI, HDMI and DisplayPort. These are the D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI and D2CIM-DVUSB-DP.
Does the Dominion KSX II provide an integrated interface that gives a view of all connected devices?	Yes. Dominion KSX II provides a single, consolidated view of all KVM and serial devices via one sign-on. A single IP address gives access to all connected serial devices. For CLI connectivity, any JAVA™-enabled web browser provides VT100/ANSI terminal emulation.
Can I access serial devices from the KSX II's local port?	Yes. From the KSX II's consolidated VGA-based local port, you can access both KVM – and serially managed devices. Serial devices can also be accessed via the serial admin port of the KSX II.
What is Absolute Mouse Synchronization?	This is a technology developed by Raritan in which mouse cursors stay in synch right out of the box. It eliminates the need to manually change the mouse settings on each target server. It is a feature supported by USB 2.0-enabled servers.
Is the Dominion KSX II Sun® "break-safe"?	Yes. The Dominion KSX II units are Sun "break-safe" for use with Sun Solaris™.
What type of remote power control capabilities does the Dominion KSX II offer?	The Dominion KSX II has two dedicated power control ports in which Raritan's Dominion PX power strips can be connected. After a simple one-time configuration step, just right click on the server name to power on, off or recycle a hung server. Note that a hard reboot provides the physical equivalent of unplugging the server from the AC power line and re-inserting the plug.
Does the KSX II have a CLI?	Yes. A comprehensive Command Line Interface is available via SSH, Telnet or the local serial port. With the CLI, the user can configure, maintain and troubleshoot the KSX II, as well as access serial devices.

Question	Answer
Can the KSX II be managed by CommandCenter® Secure Gateway (CC-SG)?	Yes. With CC-SG, customers can access and manage hundreds or even thousands of devices spread across the country, or even the world.
Flexibility and Control	
KVM-over-IP, Serial Console and Remote Power Control	Remotely access servers and networking equipment in your branch and remote offices by combining KVM-over-IP, serial and remote power control in one secure appliance. Access hundreds or thousands of remote devices when integrated with Raritan's CommandCenter® Secure Gateway (CC-SG).
Centralized Access for Remote and Branch Offices	If you have geographically dispersed equipment at branch and remote offices, the KSX II enables you to reduce travel costs, increase IT productivity, decrease mean time to repair and achieve higher service quality.
Manage Racks of KVM and Serially Managed Devices	The Dominion KSX II is also ideal for labs, computer rooms and data centers with racks containing both serially – and KVM – controlled devices.
Two Secure Hardware Appliance Models	<p>The Dominion KSX II is available in two secure hardware appliances.</p> <p>The DKSX-144 features four KVM-over-IP ports, four serial ports, two power control ports and a local port for direct access.</p> <p>The DKSX-188 features eight KVM-over-IP ports, eight serial ports, two power control ports and a local port for direct access.</p> <p>Includes a built-in modem for emergency access and dual LAN ports for reliability.</p>

Question	Answer
BIOS- Level KVM-over-IP Access	KSX II provides virtually all of the KVM-over-IP features of the award winning Dominion KX II as of Release 2.5. With the Dominion KX II as its foundation, the KSX II enables new levels of KVM-over-IP performance, reliability, usability, compatibility and security. See the Dominion KX II Features and Benefits for the complete features list. Note that the tiering (cascading) feature is not yet available for the KSX II.
Secure Console Server Access	The KSX II enables true serial access of serially-controlled equipment including networking equipment, headless servers (UNIX®, Linux®, Sun®) and other devices. Providing many serial features of the Dominion SX, the KSX II does not require expensive serial dongles, like competing solutions.
Remote Power Control	You can remotely power up, down or cycle devices connected to optional Dominion PX™ power distribution units. An administrator can power cycle a hung or crashed server with a click of the mouse. The KSX II includes two power control ports that can be connected to two Raritan PX strips.
Virtual Media	<p>Mount remote drives/media on servers in remote offices to support software installation, remote booting and diagnostics. Using virtual media, you can even remotely re-image a server in a branch office.</p> <p>The Dominion KSX II supports a wide variety of media options, including</p> <p>CD/DVD/Floppy drives, hard drives, USB drives, and ISO image files.</p>
Availability	
Dual Gigabit Ethernet Ports with Failover	Provides high availability with dual gigabit Ethernet ports for redundancy. Should one Ethernet switch or interface card fail, Dominion KSX II will automatically failover to the other port and continue operating.
Built in Modem with Dial-back	The Dominion KSX II has a built-in modem for out-of-band access if the primary network is unavailable. As an added security benefit, dial-back authentication is supported.
Security	

Question	Answer
Validated FIPS 140-2 Cryptographic Module for KVM and Serial Sessions	For government, military and other high security applications, the Dominion KSX II is the first combo digital KVM and serial switch with a validated FIPS 140-2 Cryptographic Module for enhanced encryption. Modules tested and validated as conforming FIPS 140-2 are accepted by the federal agencies of the U.S. and Canada for the protection of sensitive information. FIPS 140-2 encryption can be applied to both KVM and serial sessions.
Smart Card and CAC Authentication	The Dominion KSX II supports smart card and DoD Common Access Card (CAC) authentication at the rack, stand-alone over IP and through CC-SG. Meets U.S. Government HSPD-12, PIV and CAC directives and ISO 7816, PC/SC and CCID standards. All Dominion KSX II models support smart cards using the D2CIM-DVUSB CIMs.
256-Bit AES Encryption	The Dominion KSX II uses Advanced Encryption Standard (AES) encryption for added security. AES is a U.S. government-approved cryptographic algorithm that is recommended by the National Institute of Standards and Technology (NIST) in FIPS 197.
Configurable Strong Password Checking	The Dominion KSX II has administrator-configurable strong password checking to ensure that user created passwords meet corporate standards and are resistant to brute force hacking. The administrator can also enforce password aging and lockout after failed attempts.
Group and Port-level Permissions	Administrators can ensure that only the right people access remote IT equipment by setting permissions down to the port level. Administrators can also grant or deny virtual media and power cycling privileges on a port and user basis.

Question	Answer
RADIUS and LDAP and Active Directory® Authentication	Dominion KSX II integrates with industry-standard directory servers, such as Microsoft's Active Directory, using either the LDAP or RADIUS protocols. This allows Dominion KSX II to use pre-existing username/password databases for security.
Configurable Security Banner	For government, military and other security-conscious customers requiring a security message before user login, the KSX II can display a user-configurable banner message and require acceptance before user login.
Upload Customer-Provided SSL Certificates	You can upload digital certificates to the Dominion KSX II (self-signed or certificate authority provided) for enhanced authentication and secure communication.
Advanced KVM-over-IP Features	
High Performance, Next-Generation Video Hardware	Dominion KSX II's KVM-over-IP engine uses Raritan's next-generation technology, providing virtual at-the-rack performance. Next-generation features include ultra-fast screen refresh, 1920x1080 high-definition (HD) remote video resolution, advanced color calibration and per server video optimization.
Multiplatform CIMs Support Analog and Digital Video	<p>Dominion KSX II supports multiplatform CIMs to connect to PS/2, USB, Sun and serially controlled servers.</p> <p>Analog VGA video and new DVI, HDMI and DisplayPort digital video standards are supported.</p> <p>Dominion CIMs operate at distances of up to 150 feet from the Dominion KSX II switch, depending on server resolution.</p>
Mobile KVM Access for iPhone and iPad	Users can now access and control servers connected to the Dominion KSX II via their Apple iPhones and iPads. This provides emergency 24/7 out-of-hours access, as well as convenient everyday access for iPads enthusiasts. CC-SG Release 5.2 or later is required for this capability.

Question	Answer
Blade Server Access and Control	<p>Dominion KSX II supports popular blade server models from HP, IBM® and Dell®. It provides simple, automated and secure KVM-over-IP access (1) at the rack, (2) remotely over IP, (3) via CommandCenter Secure Gateway and (4) by modem. Blade servers are displayed by chassis with simple one-click access.</p> <p>The Dominion KSX II's blade features are available to SMB customers with no management system required. For enterprise customers, seamless blade server integration with CommandCenter Secure Gateway is available.</p>
Dual Stack IP Networking with IPv6	The Dominion KSX II provides dual stack IP networking with simultaneous support of IPv4 and IPv6.
Secure Virtual Media with 128/256-Bit Encryption	Virtual media sessions are secured using 128- or 256-bit AES. Also available is 128-bit RC4 encryption.
New Dual-USB Virtual Media CIM and USB Profiles	The dual-USB virtual media CIMs (D2CIM-DVUSB) and USB profile feature enable expanded BIOS use of virtual media drives to the broadest range of servers and BIOS versions.
Ease of Use	
Next Generation Common User Interface	The Dominion KSX II has a next generation, browser-based user interface for enhanced usability and productivity. This interface is common across the local port, remote access, management software as well as other Raritan products. This reduces training time and increases productivity.
Absolute Mouse Synchronization™	The Absolute Mouse Synchronization feature is the ultimate mouse synchronization solution. For servers with a compatible USB mouse port, there is no need to adjust the mouse settings on the target server. This reduces installation time and enhances the Dominion KSX II's plug-and-play nature. In addition, the remote and target server mouse pointers never go out of synchronization. This feature is enabled by the D2CIM-VUSB and D2CIM-DVUSB virtual media CIMs.

Question	Answer
High Definition (HD) Remote Video Resolution - 1920x1080	The Dominion KSX II supports full high-definition (HD) remote video resolution (1080p). In addition, popular widescreen formats are supported including 1600x1200, 1680x1050 and 1440x900, so you can work with today's higher resolution monitors. VGA, DVI, HDMI and DisplayPort Video are supported.
Full-Screen Video Display	With the Dominion KSX II's full-screen video display, you appear to be directly connected to the target server. You can view the full video display from the target server without window borders or toolbars. A hidden toolbar of KVM client commands is available.
Automated and Manual Bandwidth Settings	Video performance can be configured to match the available network bandwidth. With high-speed LAN access, more bandwidth is available and higher quality video information can be sent, resulting in better performance. When accessing via a limited bandwidth connection, Dominion KSX II can be configured to the limited bandwidth available.
Port Scanning and Thumbnail Views	View selected servers as a slide show and/or real-time thumbnail views. The user can select a list of servers, set the scan interval and quickly access a given server. Works remotely and locally.
PC Share Mode	Up to eight users can connect and remotely access each KVM-connected server. This feature is very useful for administrator collaboration for teamed troubleshooting.
Asian Languages – Japanese and Simplified/Traditional Chinese	The Dominion KSX II's remote HTML User Interface and the KVM Clients now support the Japanese, Simplified Chinese and Traditional Chinese languages. This is available stand-alone as well as through CC-SG.
Serial Console Capabilities	
True Serial Access	The Dominion KSX II provides true, remote serial console access to either four or eight serial devices, without the use of expensive serial dongles. Note that simultaneous access to four or eight serial ports is provided, with no blocking. In addition multiple users can connect simultaneously to a serial device.
Multiple Serial Clients	Access to serial devices is provided via the Raritan Serial Console, SSH or Telnet clients.

Question	Answer
Key Logging and History	The Dominion KSX II provides a true serial connection to network devices and serially managed equipment. This includes the ability to log serial sessions and retrieve the session history.
Copy and Paste	You can copy and paste session information between different devices.
Keyword Monitoring and Alerting	You can define, for each port, a set of keywords (port triggers). The KSX II will scan the data coming from the port, and if a keyword is encountered, it will log the event and send alerts via SNMP. This allows for monitoring and alerting of problems with remote devices even when you are not connected.
Session Disconnection Commands	Once you have timed out for inactivity, a user-defined logoff command is sent to the serial device. Improved security of user sessions results, as the next user that connects to the port will need to log in to the target with their own credentials.
Secure Chat Instant Messaging	Allows encrypted instant messaging for online collaboration with other authorized browser users and maximizes the effectiveness of a distributed workforce. Reduces time to resolve problems and allows multi-person troubleshooting.
TCP Port Addressing for Telnet and SSH	Direct port addressing to specific devices via IP address and/or TCP port number for both Telnet and SSH.
Manageability	
Remote and Local Management and Administration	You can perform all management, administration and configuration operations, using a simple graphical user interface, remotely from the convenience of your desktop or while in the data center.
Centralized Management with Raritan CommandCenter Secure Gateway	Like the rest of the Dominion series, Dominion KSX II features CommandCenter Secure Gateway integration, allowing enterprise users to consolidate all Dominion devices into a single logical system, accessible from a single IP address and under a single management interface.

Question	Answer
Remote Power Control	The Dominion KSX II has two dedicated power control ports for Raritan PDUs like the Dominion PX. This enables you to remotely power cycle IT devices from the KSX II management interface.
SNMP Management and Syslog	The Dominion KSX II SNMP agent distributes SNMP traps for important system events to SNMP management systems. SNMP traps are fully configurable by the administrator. SNMP v2 and v3 supported. Syslog is also supported.
Plug-and-Play Appliance Offers Quick and Easy Setup	Dominion KSX II is a completely self-contained system (i.e. an appliance). All KSX II features, including authentication and Web access are built into the unit and do not require the use of an additional server.
Command Line Interface	A comprehensive Command Line Interface is available via SSH, Telnet or the local serial port. With the CLI, the user can configure, maintain and troubleshoot the KSX II, as well as connect to serial devices.

Index

A

- A. AC Power • 12
- About the Virtual KVM Client • 47
- Absolute Mouse Synchronization • 61
- Access a Virtual Media Drive on a Client Computer • 87
- Access and Control Target Servers Remotely • 21
- Access and Display Favorites • 41
- Access the Port Configuration Page • 128
- Accessing a Target Server • 22, 247
- Accessing Telnet from a Windows PC • 233
- Accessing the KSX II Using CLI • 232
- Accessing Virtual Media on a Windows 2000 • 315
- Active KVM Client (AKC) • 30, 73
- Active System Partition • 90
- Active System Partitions • 89
- Adding a New User • 107
- Adding a New User Group • 101, 107
- Adding Attributes to the Class • 305
- Adding Scripts • 184
- Additional Security Warnings • 23, 24
- Adjusting Video Settings • 57
- Administering the KSX II Console Server Configuration Commands • 241
- AES 256 Prerequisites and Supported Configurations for Java • 311
- AKC Download Server Certification Validation IPv6 Support Notes • 314
- AKC Supported Browsers • 75
- AKC Supported Microsoft .NET Framework • 74
- AKC Supported Operating Systems • 75
- Allow Cookies • 75
- Allow Pop-Ups • 23
- Apple Mac Mouse Settings • 11
- Apply a Native Display Resolution to Other CIMs • 4, 134
- Apply Selected Profiles to Other CIMs • 133
- Applying and Removing Scripts • 184, 187
- Assign the KSX II an IP Address • 18, 125
- Assigning a Name to the PX • 135
- Associating KVM and Serial Target Servers to Outlets (Port Page) • 135
- Audit Log • 212, 259, 260
- Authentication Settings • 111

- Authentication When Accessing a Smart Card Reader • 65

- Auto-Sense Video Settings • 57
- Available Resolutions • 247
- Available USB Profiles • 93, 318

B

- B. Network Port • 13
- Backup and Restore • 150, 191, 214
- Blade Chassis - Port Access Page • 37
- Blade Chassis Sample URL Formats • 144, 157
- Browser Notes • 323
- Build a New Macro • 54

C

- C. Local User Port (Local PC) and Local Admin Port • 14
- Calibrating Color • 57
- CC Unmanage • 221
- CC-SG Notes • 323
- Certified Modems for UNIX, Linux and MPC • 261
- Change the Default Password • 17
- Changing a Password • 123
- Changing a USB Profile when Using a Smart Card Reader • 319
- Changing the Default GUI Language Setting • 192
- Changing the Keyboard Layout Code (Sun Targets) • 23
- Changing the Maximum Refresh Rate • 60
- Checking Your Browser for AES Encryption • 199, 200, 201
- Choosing USB Profiles • 49
- CIM Compatibility • 93
- CIM Notes • 315
- CIMs Required for Virtual Media • 84
- Cisco ACS 5.x for RADIUS Authentication • 119
- CLI Commands • 231, 239
- CLI Prompts • 239
- CLI Syntax -Tips and Shortcuts • 237
- Client Dial-Up Networking Configuration • 263
- Client Launch Settings • 70
- Command Line Interface (CLI) • 30, 230
- Common Commands for All Command Line Interface Levels • 237

- Completion of Commands • 236
- Conditions when Read/Write is Not Available • 85, 87
- Configure Date/Time Settings (Optional) • 20
- Configure Scan Settings in VKC and AKC • 43, 71
- Configure the CIM Power Associations • 133
- Configure the CIM Settings • 132
- Configure the CIM Target Settings • 133
- Configure the DNS Settings • 19, 127
- Configure the IPv4 Settings • 18, 125
- Configure the IPv6 Settings • 19, 126
- Configuring Blade Chassis • 137
- Configuring CIM Ports • 132, 279, 281, 301
- Configuring Date/Time Settings • 174, 206
- Configuring Direct Port Access via Telnet, IP Address or SSH • 167
- Configuring Event Management - Destinations • 173, 175, 177, 182
- Configuring Event Management - Settings • 175, 182
- Configuring IP Access Control • 204
- Configuring KSX II Local Port Settings • 160
- Configuring KVM Switches • 131
- Configuring Modem Settings • 173
- Configuring Network • 241
- Configuring Ports • 128
- Configuring SNMP Agents • 171, 176
- Configuring SNMP Traps • 173, 175, 176
- Configuring USB Profiles (Port Page) • 99, 147, 158
- Connect and Disconnect Scripts • 183
- Connect Commands • 243
- Connect Key Examples • 161, 252
- Connect to a Target Server • 74
- Connecting and Disconnecting from Virtual Media • 87
- Connecting to a KVM Target Server • 47, 49
- Connection Information • 52
- Connection Properties • 50
- Connectivity • 287, 288
- Creating a New Attribute • 304
- Creating Port Groups • 191

D

- D. KVM Target Server Ports • 14
- DB25F Nulling Serial Adapter Pinouts • 296
- DB25M Nulling Serial Adapter Pinouts • 296
- DB9F Nulling Serial Adapter Pinouts • 295
- DB9M Nulling Serial Adapter Pinouts • 295
- Default Login Information • 8

- Dell Blade Chassis Configuration • 141
- Dell Chassis Cable Lengths and Video Resolutions • 139, 141, 145, 315
- Dell OptiPlex and Dimension Computers • 315
- Device Diagnostics • 228
- Device Information • 213
- Device Management • 124
- Device Services • 163
- Diagnostics • 224
- Digital CIM Display Native Resolution • 281
- Digital CIM Established and Standard Modes • 280, 281
- Digital CIM Target Server Timing and Video Resolution • 278
- Digital CIM Timing Modes • 279
- Digital Video CIMs for Macs • 281
- Direct Port Access URL Syntax for the Active KVM Client (AKC) • 166
- Direct Port Access URL Syntax for the Virtual KVM Client (VKC) • 165
- Disable 'Protected Mode' • 76
- Disconnect from Virtual Media Drives • 89
- Disconnecting a Target Server • 22
- Disconnecting KVM Target Servers • 48
- Disconnecting Users from Ports • 109, 110
- Discovering Devices on the KSX II Subnet • 42
- Discovering Devices on the Local Subnet • 41
- Drive Partitions • 90
- Dual Mouse Modes • 61
- DVI Compatibility Mode • 281

E

- E. Power Strip • 15
- Editing rcusergroup Attributes for User Members • 307
- Emergency Connectivity • 288
- Enable AKC Download Server Certificate Validation • 76
- Enable Direct Port Access • 167
- Enable Favorites • 40
- Enabling Direct Port Access via URL • 165
- Enabling FIPS 140-2 • 200, 202
- Enabling Serial Console Access • 164
- Enabling SSH • 163
- Enabling Telnet • 163, 233
- Enabling the AKC Download Server Certificate Validation • 170
- Encryption & Share • 199, 203, 260
- Enter Intelligent Mouse Mode • 61
- Entering the Discovery Port • 164

Event Management • 175
 Example 1
 Import the Certificate into the Browser • 25, 28
 Example 2
 Add the KSX II to Trusted Sites and Import the Certificate • 27
 Export Macros • 56

F

F. Serial Target Ports • 16
 FAQs • 325
 FIPS 140-2 Support Requirements • 203
 French Keyboard • 319
 From LDAP/LDAPS • 303
 From Microsoft Active Directory • 303
 Full Screen Mode • 73

G

General Settings • 67
 Generic Blade Chassis Configuration • 139
 Getting Started • 8
 Group-Based IP ACL (Access Control List) • 102, 104

H

Handling Conflicts in Profile Names • 217
 Hardware • 6, 274
 Help Choosing USB Profiles • 317
 Hot Keys and Connect Keys • 252
 HP and Cisco UCS Blade Chassis Configuration (Port Group Management) • 150, 152, 191
 HTTP and HTTPS Port Settings • 164, 289

I

IBM AIX Mouse Settings • 12
 IBM Blade Chassis Configuration • 145
 Implementing LDAP/LDAPS Remote Authentication • 111, 112
 Implementing RADIUS Remote Authentication • 111, 116
 Import Macros • 55
 Importing and Exporting Scripts • 184, 187
 Include KSX II IP Address in 'Trusted Sites Zone' • 75
 Informational Notes • 311
 Initial Configuration Using CLI • 238
 Installation and Configuration • 8
 Installing a Certificate • 4, 23, 24
 Intelligent Mouse Mode • 61

Intelligent Mouse Synchronization Conditions • 62
 Interface and Navigation • 33
 Interface Command • 242
 Interfaces • 29
 Introduction • 1
 IPv6 Command • 244
 IPv6 Support Notes • 314

J

Java Not Loading Properly on Mac • 313
 Java Runtime Environment (JRE) • 312
 Java Runtime Environment (JRE) Notes • 311
 Java Validation and Access Warning • 23
 JRE Requirements and Browser Considerations for Mac • 299

K

Key Combinations and the Java Runtime Environment (JRE) • 322
 Keyboard • 52
 Keyboard Language Preference (Fedora Linux Clients) • 321
 Keyboard Limitations • 69
 Keyboard Macros • 53
 Keyboard Notes • 319
 KSX II Client Applications • 5
 KSX II Console Navigation • 35
 KSX II Dimensions and Physical Specifications • 274
 KSX II Electrical Specifications • 275
 KSX II Environmental Requirements - KSX II • 274
 KSX II FAQs • 325
 KSX II Help • 7
 KSX II Interface • 33
 KSX II Local Console • 245
 KSX II Devices • 30
 KSX II Local Console Factory Reset • 259
 KSX II Local Console Interface • 246
 KSX II Local Console Local Port Settings • 256
 KSX II Overview • 2
 KSX II Remote Console Interface • 30, 31
 KSX II Serial RJ-45 Pinouts • 294
 KSX II Supported Keyboard Languages • 254, 301
 KSX II Virtual Media Prerequisites • 83
 KSX II-to-KSX II Paragon CIM Guidelines • 283
 KSX II-to-Paragon II Guidelines • 284

KVM Properties • 275

L

LAN Interface Settings • 124, 127
 Launching MPC from a Web Browser • 76
 Launching MPC on Mac Lion Clients • 77
 Launching the KSX II Remote Console • 31
 Left Panel • 34
 Linux Mouse Settings • 11
 List of KSX II SNMP Traps • 173, 176, 178
 Local Console Smart Card Access • 64, 249
 Local Console USB Profile Options • 250
 Local Port Administration • 256
 Local Port Requirements • 290
 Local Port Scan Mode • 249
 Local Serial Port Connection to the KSX II • 233
 Logging On • 234
 Logging Out • 45
 Logging Users Off the KSX II (Force Logoff) • 109, 110
 Login Limitations • 193, 194
 Low Bandwidth KVM Settings • 262

M

Mac Keyboard Keys Not Supported for Remote Access • 322
 Mac Mini BIOS Keystroke Commands • 293
 Maintenance • 211
 Maintenance Features (Local/Remote Console) • 211
 Managing Favorites • 4, 35, 39, 74
 Modem Configuration • 261
 Modifying an Existing User • 110
 Modifying an Existing User Group • 106
 Modifying Scripts • 187
 Mount a Smart Card Reader • 66
 Mounting CD-ROM/DVD-ROM/ISO Images • 88, 91
 Mounting Local Drives • 84
 Mouse Modes when Using the Mac Boot Menu • 96, 99, 158
 Mouse Options • 60
 Mouse Pointer Synchronization (Fedora) • 324
 Mouse Settings • 9
 Mouse Synchronization Tips • 63
 Moving Between Ports on a Device • 323
 Multi-Platform Client (MPC) • 30, 76

N

Name Command • 242
 Name Your Target Servers • 20
 Navigation of the CLI • 235, 236
 Network Basic Settings • 125
 Network Interface Page • 224
 Network Settings • 4, 124, 125, 289
 Network Speed Settings • 127, 286
 Network Statistics Page • 224
 Non-US Keyboards • 319
 Notes on Mounting Local Drives • 84
 Number of Supported Virtual Media Drives • 86

O

Opening RSC from the Remote Console • 78
 Operating System IPv6 Support Notes • 314
 Overview • 8, 74, 80, 92, 231, 245, 311

P

Package Contents • 4
 PC Share Mode and Privacy Settings when Using Smart Cards • 65
 Permissions • 102, 103
 Ping Host Page • 226
 Port Access Page (Local Console Server Display) • 247
 Port Access Page (Remote Console Display) • 36
 Port Action Menu • 37, 38
 Port Configuration Page • 129
 Port Group Management • 191
 Port Keywords • 189
 Port Name • 130
 Port Number • 129
 Port Permissions • 102, 104
 Port Settings • 234
 Port Sharing Using CLI • 241
 Port Type • 130
 Power Control • 134
 Power Controlling a Target Server • 48
 Prerequisites for Using AKC • 74, 75
 Prerequisites for Using Virtual Media • 83
 Product Features • 6
 Product Photos • 5
 Proxy Server Configuration for Use with MPC, VKC and AKC • 45

R

- Rack PDU (Power Strip) Outlet Control • 80
- RADIUS Communication Exchange
 - Specifications • 120
- Raritan Serial Console (RSC) • 30, 78
- Rebooting the KSX II • 220
- Refreshing the Screen • 56
- Relationship Between Users and Groups • 101
- Remote Client Requirements • 291
- Remote PC VM Prerequisites • 84
- Required and Recommended Blade Chassis Configurations • 139, 141, 145, 155
- Resetting the KSX II Using the Reset Button • 260
- Resolving Fedora Core Focus • 323
- Resolving Issues with Firefox Freezing when Using Fedora • 324
- Returning to the KSX II Local Console Interface • 255
- Returning User Group Information • 303
- Returning User Group Information from Active Directory Server • 115
- Returning User Group Information via RADIUS • 120
- Root User Permission Requirement • 90

S

- Scaling • 72
- Scanning Ports • 43
- Scanning Ports - Local Console • 248
- Screenshot from Target Command (Target Screenshot) • 59
- Security and Authentication • 246
- Security Banner • 209
- Security Issues • 240
- Security Management • 193
- Security Settings • 83, 107, 193
- Security Warnings and Validation Messages • 23, 24
- Selecting Profiles for a KVM Port • 99
- Send Ctrl+Alt+Del Macro • 52
- Send LeftAlt+Tab (Switch Between Open Windows on a Target Server) • 52
- Send Smart Card Remove and Reinsert Notifications • 66
- Send Text to Target • 53
- Server Display • 251
- Set Scan Tab • 38
- Setting CIM Keyboard/Mouse Options • 53
- Setting Emulation on a Target • 240

- Setting Network Parameters • 238
- Setting Parameters • 238
- Setting Permissions for an Individual Group • 102, 108
- Setting the Registry to Permit Write Operations to the Schema • 304
- Simultaneous Users • 245
- Single Mouse Mode • 64
- Single Mouse Mode when Connecting to a Target Under CC-SG Control • 323
- Smart Card Minimum System Requirements • 65, 249, 290
- Smart Card Minimum System Requirements, CIMs and Supported/Unsupported Smart Card Readers • 64, 65
- Smart Card Reader Detected • 65
- Smart Card Reader Not Detected when Using a DVM-DP CIM • 315
- Smart Cards • 64
- Software • 7, 297
- Special Sun Key Combinations • 255
- Specifications • 2, 274
- SSH Access from a UNIX/Linux Workstation • 232
- SSH Access from a Windows PC • 232
- SSH Connection to the KSX II • 232
- SSL Certificates • 23, 206
- Standard Mouse Mode • 62
- Step 1
 - Configure the KVM Target Servers • 9
- Step 2
 - Configure Network Firewall Settings • 12
- Step 3
 - Connect the Equipment • 12
- Step 4
 - Configure the KSX II • 17
- Step 5
 - Launching the KSX II Remote Console • 21
- Step 6
 - Configuring the Keyboard Language (Optional) • 22
- Stopping CC-SG Management • 222
- Strong Passwords • 123, 193, 196
- Sun Solaris Mouse Settings • 11
- Supported and Unsupported Smart Card Readers • 65, 249, 292
- Supported Blade Chassis Models • 152
- Supported Browsers • 298
- Supported CIMs for Blade Chassis • 152
- Supported Computer Interface Module (CIMs) Specifications • 276
- Supported Distances for Serial Devices • 287

- Supported Operating Systems (Clients) • 297
- Supported Paragon II CIMS and Configurations • 201, 282
- Supported Remote Connections • 285
- Supported Target Server Video Resolution/Refresh Rate/Connection Distance • 275
- Supported Tasks Via Virtual Media • 85
- Supported Video Resolutions • 276, 299
- Supported Virtual Media Operating Systems • 86
- Supported Virtual Media Types • 85
- SUSE/VESA Video Modes • 324
- Switching Between KVM Target Servers • 47
- Switching between Target Servers • 22
- Synchronize Your Mouse • 63
- SysLog Configuration • 182

T

- Target BIOS Boot Time with Virtual Media • 316
- Target Connections and the CLI • 240
- Target Server Requirements • 290
- Target Server Video Resolutions • 9
- Target Server VM Prerequisites • 84
- TCP and UDP Ports Used • 288
- TCP Port 443 • 12
- TCP Port 5000 • 12
- TCP Port 80 • 12
- Telnet Connection to the KSX II • 233
- Tips for Adding a Web Browser Interface • 140, 143, 144, 147, 148, 149
- Tool Options • 67, 73
- Trace Route to Host Page • 227
- Turning Outlets On/Off and Cycling Power • 81

U

- Unmount (Remove) a Smart Card Reader • 66
- Update a Smart Card Reader • 66
- Updating the LDAP/LDAPS Schema • 303
- Updating the Schema Cache • 307
- Upgrade History • 220
- Upgrading CIMS • 217
- Upgrading Firmware • 217
- USB Port and Profile Notes • 316
- USB Profile Management • 216, 217
- USB Profiles • 49, 92, 158
- User Authentication Process • 122
- User Blocking • 193, 197

- User Group List • 101
- User Groups • 100
- User Management • 100
- Users • 107
- Using a Windows Keyboard to Access Mac Targets • 294
- Using Scan Port Options • 44
- Using the KSX II Local Console • 245

V

- Version Information - Virtual KVM Client • 73
- Video Image Appears Dark when Using a Mac • 301
- Video Properties • 56
- View by Group Tab • 37
- View by Search Tab • 37
- View KSX II User List • 108
- View Options • 72
- View Status Bar • 72
- View Toolbar • 72
- View Users by Port • 108, 109
- Viewing the KSX II MIB • 171, 176, 181
- Virtual KVM Client (VKC) • 30, 38, 46, 92
- Virtual KVM Client Java Requirements • 47
- Virtual KVM Client Version Not Known from CC-SG Proxy Mode • 323
- Virtual Media • 83
- Virtual Media Connection Failures Using High Speed for Virtual Media Connections • 316
- Virtual Media File Server Setup (File Server ISO Images Only) • 91
- Virtual Media in a Linux Environment • 89
- Virtual Media in a Mac Environment • 90
- Virtual Media in a Windows XP Environment • 89
- Virtual Media Not Refreshed After Files Added • 316
- Virtual Media Notes • 315
- VKC and MPC Smart Card Connections to Fedora Servers • 324
- VM-CIMS and DL360 USB Ports • 316

W

- What's New in Help • 4
- Windows 2000 Dial-Up Networking Configuration • 263
- Windows 2000 Mouse Settings • 10
- Windows 3-Button Mouse on Linux Targets • 315

Windows 7 and Windows Vista Mouse
Settings • 10
Windows Vista Dial-Up Networking
Configuration • 267
Windows XP Dial-Up Networking
Configuration • 268
Windows XP, Windows 2003, Windows 2008
Mouse Settings • 10
Working with Target Servers • 29

► U.S./Canada/Latin America

Monday - Friday
8 a.m. - 6 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

► China

Beijing

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

► India

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

► Japan

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-5795-3170
Email: support.japan@raritan.com

► Europe

Europe

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom

Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany

Monday - Friday
8:30 a.m. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

► Melbourne, Australia

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

► Taiwan

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com