



# **Dominion KSX II**

## **User Guide**

### **Release 1.0.0**

Copyright © 2008 Raritan, Inc.  
DKSXII-0B-E  
January 2008  
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 2007 Raritan, Inc., CommandCenter®, Dominion®, Paragon® and the Raritan company logo are trademarks or registered trademarks of Raritan, Inc. All rights reserved. Java® is a registered trademark of Sun Microsystems, Inc. Internet Explorer® is a registered trademark of Microsoft Corporation. Netscape® and Netscape Navigator® are registered trademarks of Netscape Communication Corporation. All other trademarks or registered trademarks 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.



# Contents

## Chapter 1

---

### **Introduction** **1**

---

Dominion KSX II Overview .....	2
Virtual Media .....	4
Product Photos .....	5
Product Features .....	6
Hardware .....	6
Software .....	7
Terminology .....	7
External Product Overview .....	9
Package Contents .....	12
User Guide .....	12
Organization of Information .....	13
Related Documentation .....	14

### **Getting Started** **15**

---

Login Information .....	15
Default IP Address .....	15
Supported Operating Systems (Clients) .....	15
Supported Browsers .....	16
Supported Operating Systems and CIMs (KVM Target Servers) .....	16

### **Installation and Configuration** **19**

---

Overview .....	19
Step 1: Configure KVM Target Servers .....	19
Supported Video Resolutions .....	20
Desktop Background .....	20
Mouse Settings .....	21
Operating System Mouse and Video Settings .....	21
Windows XP / Windows 2003 Settings .....	21
Windows 2000 Settings .....	22
Windows Vista .....	23
Linux Settings (Red Hat 9) .....	24
Linux Settings (Red Hat 4) .....	26

## Contents

SUSE Linux 10.1 Settings .....	26
Make Linux Settings Permanent .....	27
Make UNIX Settings Permanent .....	28
Sun Solaris Settings .....	28
IBM AIX 5.3 Settings .....	31
Apple Macintosh Settings.....	32
Step 2 (Optional): Configure Keyboard Language .....	32
Change the Keyboard Layout Code (Sun Targets) .....	32
Step 3: Configure Network Firewall Settings.....	33
Step 4: Connect the Equipment.....	34
1. AC Power .....	34
2. Network Ports.....	34
3. Local User Port (local PC) and Local Admin Port.....	35
4. KVM Target Server Ports .....	35
5. Power Strip .....	36
6. Serial Target Ports .....	36
Step 5: KSX II Initial Configuration .....	38
Changing the Default Password .....	38
Assign an IP Address.....	39
Configure Direct Port Access .....	40
Configure KVM and Serial Ports.....	42
Remote Authentication.....	48
Users, Groups, Relationships and Access Permissions.....	52

## Connecting to the KSX II

**54**

User Interfaces.....	54
KSX II Local Console: KSX II Devices.....	55
Multi-Platform Client (MPC) .....	55
Language Support.....	56
Java Runtime Environment (JRE) .....	57
Launching the KSX II.....	57
KSX II Console Layout.....	59
KSX II Console Menus .....	59
Logging Out.....	62
Managing Favorites .....	62
Favorites List .....	65
Discover Devices - Local Subnet .....	67
Discover Devices - KSX II Subnet.....	69
Add New Favorite.....	70

**Accessing Target Servers 72**

---

Port Access Page .....73

Port Action Menu - KVM and Serial Ports .....75

Connecting to a KVM Target Server .....76

Connecting to a Serial Target Server .....77

Switching Between KVM Target Servers.....77

Disconnecting KVM and Serial Targets.....77

Power Controlling a Target Server .....78

    Power Cycle a Target Server .....78

    Power On a Target Server.....79

    Power Off a Target Server .....80

**Virtual KVM Client 81**

---

Overview .....82

Options .....83

    Menu Tree.....83

    Toolbar .....84

Mouse Pointer Synchronization.....85

    Mouse Synchronization Tips .....85

Connection Menu.....87

    Properties Dialog.....87

    Connection.....89

    Exit .....90

Keyboard Menu .....90

    Send Ctrl+Alt+Delete .....90

    Set CIM Keyboard/Mouse Options .....90

    Keyboard Macros .....91

    Creating a Keyboard Macro .....92

    Running a Keyboard Macro .....94

    Modifying a Keyboard Macro .....94

    Removing a Keyboard Macro.....94

Video Menu.....95

    Refresh Screen .....95

    Auto-sense Video Settings.....95

    Calibrate Color .....96

    Video Settings.....96

Mouse Menu.....99

    Synchronize Mouse.....99

    Single Mouse Cursor.....100

    Standard.....100

    Intelligent.....101

    Absolute.....101

## Contents

Virtual Media .....	101
Tools Menu.....	102
Options.....	102
View Menu .....	103
View Toolbar .....	103
Scaling.....	103
Target Screen Resolution .....	104
Help Menu.....	104
About Raritan Virtual KVM Client .....	104

## Virtual Media 105

---

Overview .....	106
Prerequisites for Using Virtual Media.....	108
Using Virtual Media .....	109
Opening a KVM Session.....	110
Connecting to Virtual Media.....	112
Local Drives.....	112
Conditions when Read-Write is not Available.....	113
CD-ROM/DVD-ROM/ISO Images .....	114
Disconnecting Virtual Media .....	115
File Server Setup (File Server ISO Images Only).....	116

## User Management 118

---

User Management Menu.....	118
User List.....	119
Adding a New User.....	120
Modify Existing User .....	121
User Group List.....	122
Add New User Group .....	123
Setting Permissions .....	125
Setting Port Permissions .....	126
Group-based IP ACL (Access Control List).....	126
Modify Existing User Group .....	129
Set Permissions for Individual Group .....	131
Change Password .....	131
Authentication Settings .....	132
Implementing LDAP Remote Authentication.....	135
Returning User Group Information from Active Directory Server.....	137
Implementing RADIUS Remote Authentication.....	138
Returning User Group Information via RADIUS.....	139
RADIUS Communication Exchange Specifications .....	139

**Device Management** **141**

---

- Device Settings Menu ..... 141
- Network Settings ..... 142
  - Network Basic Settings ..... 143
  - LAN Interface Settings..... 145
- Device Services..... 146
- Modem Settings ..... 148
- Date/Time Settings..... 149
- Event Management ..... 150
  - Event Management - Settings..... 151
  - Event Management - Destinations ..... 153
- Port Configuration Page..... 158
  - Power Control ..... 159
  - Port Keywords..... 165

## Contents

### **Security Settings** **168**

---

Security Settings Menu .....	169
Login Limitations .....	170
Strong Passwords .....	171
User Blocking .....	172
Encryption & Share .....	173
Checking Your Browser for AES Encryption .....	176
IP Access Control .....	176

### **Maintenance** **179**

---

Maintenance Menu .....	179
Maintenance Features (Local/Remote Console) .....	179
Audit Log .....	180
Device Information .....	181
Backup and Restore .....	182
CIM Upgrade .....	184
Firmware Upgrade .....	185
Upgrade History .....	187
Reboot .....	187

### **Diagnostics** **189**

---

Diagnostics Menu .....	189
Network Interface Page .....	190
Network Statistics Page .....	190
Ping Host Page .....	193
Trace Route to Host Page .....	194
Device Diagnostics .....	195

### **KSX II Local Console** **197**

---

Reset Button .....	198
Physical Connections .....	198
Starting the KSX II Local Console .....	199
Simultaneous Users .....	199
Security and Authentication .....	199
KSX II Local Console Interface .....	200
Available Resolutions .....	200



Server Display .....	200
Hotkeys.....	201
Accessing a Target Server.....	201
Returning to the KSX II Local Console Interface .....	202
Local Port Administration.....	202
Local Port Settings (KSX II Local Console Only).....	203
Factory Reset (KSX II Local Console Only) .....	206

## **Raritan Serial Console 208**

---

System Requirements .....	208
Setting Windows OS Variables.....	208
Setting Linux OS Variables.....	212
Setting UNIX OS Variables.....	212
Installing RSC on Windows .....	213
Installing RSC for Sun Solaris and Linux .....	215
Launching RSC from a KSX II Remote Console.....	216
Raritan Serial Client Interface .....	217
Default RSC Option Values .....	219
Emulator .....	219
Edit.....	228
Tools.....	229
Chat.....	232
Help.....	232

## **Command Line Interface (CLI) 234**

---

Overview .....	234
Accessing the KSX II Using CLI.....	235
SSH Connection to the KSX II.....	236
SSH Access from a Windows PC.....	236
SSH Access from a UNIX Workstation.....	236
Telnet Connection to the KSX II.....	236
Enabling Telnet.....	237
TELNET Access from a Windows PC.....	237
Local Serial Port Connection to the KSX II.....	237
Port Settings.....	238
Login.....	238
Navigation of the CLI.....	240
Completion of Command.....	240
CLI Syntax -Tips and Shortcuts.....	241
Common Commands for all Command Line Interface Levels.....	241
Initial Configuration .....	242
Setting Parameters .....	242
Setting Network Parameters.....	242

## Contents

CLI Prompts .....	243
CLI Commands .....	243
Security Issues .....	244
Target Connections and the CLI .....	244
Set Emulation on Target .....	244
Port Sharing Using CLI .....	245
Administering the KSX II Console Server Configuration Commands .....	245
Configuring Network .....	245
Interface Command .....	246
Name Command .....	246
Connect Commands .....	247

## **CC Unmanage** **248**

---

Overview .....	248
Removing KSX II from CC-SG Management .....	249

## **Modem Configuration** **251**

---

Certified Modems for UNIX, Linux and MPC .....	251
Client Dial-Up Networking Configuration .....	251
Windows NT Dial-Up Networking Configuration .....	251
Windows 2000 Dial-Up Networking Configuration .....	254
Windows XP Dial-Up Networking Configuration .....	258

## **Specifications** **265**

---

Environmental Requirements .....	265
Physical Specifications .....	266
Computer Interface Modules (CIMs) .....	266
Emergency Connectivity .....	267
Electrical Specifications .....	267
Remote Connection .....	268
KVM Properties .....	268
Ports Used .....	269
Target Server Connection Distance and Video Resolution .....	270
Distances for Serial Devices .....	270
Network Speed Settings .....	271
Connectivity .....	272
KSX II Serial RJ-45 Pinouts .....	273
DB9F Nulling Serial Adapter Pinouts .....	274
DB9M Nulling Serial Adapter Pinouts .....	274
DB25F Nulling Serial Adapter Pinouts .....	274
DB25M Nulling Serial Adapter Pinouts .....	275

**Updating the LDAP/LDAPS Schema 276**

---

Returning User Group Information.....276  
     From LDAP.....276  
     From Microsoft Active Directory .....277  
 Setting the Registry to Permit Write Operations to the Schema .....277  
 Creating a New Attribute.....278  
 Adding Attributes to the Class .....279  
 Updating the Schema Cache .....280  
 Editing rcusergroup Attributes for User Members .....281

**Informational Notes 285**

---

Overview .....285  
 AES\_256 Support for Java Clients.....286  
 Non-US Keyboards.....287  
     French Keyboard.....287  
     Java Runtime Environment (JRE).....289  
     Keyboard Language Preference (Fedora Linux Clients).....289  
 Macintosh Keyboard.....290  
 Mouse Pointer Synchronization (Fedora).....290  
 Resolving Fedora Core Focus.....291  
 SUSE/VESA Video Modes.....291  
 CIMs.....292  
     Windows 3-Button Mouse on Linux Targets.....292  
 Virtual Media .....292  
     Dell OpTipler and Dimension Computers.....292  
     Virtual Media not Refreshed after Files Added .....292  
     Target BIOS Boot Time with Virtual Media .....292  
 CC-SG.....293  
     Virtual KVM Client Version not Known from CC-SG Proxy Mode .....293  
     Proxy Mode and MPC.....293

**FAQs 294**

---

General Questions.....294  
     What is KSX II?.....294  
     How does KSX II differ from remote control software? .....295  
     How do the new features of the KSX II compare to the KSX I? .....295  
     How do I migrate from the Dominion KSX I to KSX II?.....295  
     What CIMs are support for the KSX II switch? .....295  
     Can the KSX II be rack mounted? .....295  
     How large is the KSX II?.....296

## Contents

Serial Access .....	296
My Dominion KSX II has just been configured with a network address and I can successfully ping the IP, but when I try to access it using a web browser, the message reads "Page cannot be found or server error, please contact System Administrator." .....	296
When I select the "Send Break" option from the Emulator menu in Raritan Console (on my DSX), it does not send a break to my Sun server. What could be wrong and how can I address it? .....	296
How can I consolidate the sites where I have a Dominion KSX II installed?.....	296
Is the Ethernet port on the KSX II unit 10/100/1000 Mbps auto sensing? .....	296
Does Dominion KSX II support RS422 and RS485? .....	297
I have a server/serially managed device that is more than 300 feet from the KSX II - how do I connect? .....	297
Does Dominion KSX II support RS422 and RS485? .....	297
Can I open multiple windows and "tile" to monitor multiple servers and other IT equipment? .....	297
I manage many servers. How do I select a server to connect to?.....	297
As a user, do I see all servers connected to a Dominion KSX II? .....	298
Does Dominion KSX II work with Raritan's CommandCenter™? .....	298
Is the modem used only for administering the Dominion KSX II itself?.....	298
Is a modem standard on any Dominion KSX II models?.....	298
What level of control does Dominion KSX II have over attached target servers? .....	298
Why do I need to use a serial adapter to connect to some servers? .....	298
Is the Dominion KSX II unit SUN "break-safe"?.....	298
I have lost my Admin password to the Dominion KSX II. Is there a back door or secret password? .....	299
What remote access connection methods can KSX II accommodate?.....	299
Which ports need to be open on the corporate firewall for a secure console session using Dominion KSX II?.....	299
How do I get access to the operating system of the KSX II?.....	299
I have a few serial devices located a distance away from my server closet and the Dominion KSX II. Can I connect these devices to my Raritan switch?.....	299
How do I upgrade the software on my Dominion KSX II? .....	299
Are updates to Dominion KSX II software free? .....	300
Does Dominion KSX II require any additional client software? .....	300
What is the name of the terminal emulation package included with Dominion KSX II?.....	300
What Authentication mechanisms does the Dominion KSX II support? .....	300
Does Dominion KSX II support SNMP? .....	300
Does Dominion KSX II support syslog? .....	300
Can I log every keystroke of a session (input from user and response from a server/device) with a server?.....	300
Does Dominion KSX II support TELNET? .....	300
Can I send an intentional "break" signal to the SUN Solaris server when using SSH?.....	301
Can I send an intentional "break" signal to the SUN Solaris server when using a web browser?.....	301
Can I send an intentional "break" signal to the SUN Solaris server when using TELNET?.....	301
Can I get the buffered off-line data from a serial port when using SSH? .....	301

## Contents

Can I get the buffered off-line data from a serial port when using telnet?.....	301
Can I use KSX II over a VPN connection? .....	301
Can I get the buffered off-line data from a serial port when using a Java-enabled web-browser?.....	301
Does Dominion KSX II support local (direct) port access for "crash-cart" applications in a data center?.....	301
What are the pin-outs of the Dominion KSX II serial ports? .....	302
What web browsers have you tested with?.....	302
The Dominion KSX II uses the web browser to access serial devices. What are the advantages of Java-enabled web browser access? .....	303
Remote Access.....	304
How many users can remotely access servers on each KSX II? .....	304
Can two people look at the same server at the same time? .....	304
Can two people access the same server, one remotely and one from the local port? .....	304
In order to access KSX II from a client, what hardware, software or network configuration is required?.....	304
What is the file size of the virtual KVM client applet that is used to access KSX II? How long does it take to retrieve?.....	305
How do I access servers connected to KSX II if the network ever becomes unavailable?.....	305
Do you have a non-Windows client? .....	305
Sometimes during a Virtual KVM Client session, the Alt key appears to get stuck. What should I do? .....	305
Universal Virtual Media .....	306
What KSX II models support virtual media? .....	306
What types of virtual media does the KSX II support? .....	306
What is required for virtual media?.....	306
Is virtual media secure? .....	306
Ethernet and IP Networking .....	306
Does the KSX II offer dual gigabit Ethernet ports to provide redundant fail-over, or load balancing? .....	306
How much bandwidth does KSX II require? .....	307
What is the slowest connection (lowest bandwidth) over which KSX II can operate? .....	307
What is the speed of KSX II's Ethernet interfaces? .....	308
Can I access KSX II over a wireless connection? .....	308
Can KSX II be used over the WAN (Internet), or just over the corporate LAN? .....	308
How many TCP ports must be open on my firewall in order to enable network access to KSX II? Are these ports configurable? .....	308
Can KSX II be used with CITRIX? .....	308
Does KSX II require an external authentication server to operate? .....	309
Can the KSX II use DHCP? .....	309
I'm having problems connecting to the KSX II over my IP network. What could be the problem? .....	309
Servers .....	310
Does KSX II depend on a Windows server to operate? .....	310

## Contents

Do I need to install a web server such as Microsoft Internet Information Services (IIS) in order to use KSX II's web browser capability? .....	310
What software do I have to install in order to access KSX II from a particular workstation? .....	310
Installation .....	310
Besides the unit itself, what do I need to order from Raritan to install KSX II? .....	310
What kind of Cat5 cabling should be used in my installation? .....	310
What types of servers can be connected to KSX II? .....	311
How do I connect servers to KSX II? .....	311
How far can my servers be from KSX II? .....	311
Some operating systems lock up when I disconnect a keyboard or mouse during operation. What prevents servers connected to KSX II from locking up when I switch away from them? .....	311
Are there any agents that must be installed on servers connected to KSX II? .....	311
How many servers can be connected to each KSX II unit? .....	311
What happens if I disconnect a server from KSX II and reconnect it to another KSX II unit, or connect it to a different port on the same KSX II unit? .....	312
Local Port .....	312
Can I access my servers directly from the rack? .....	312
When I am using the local port, do I prevent other users from accessing servers remotely? .....	312
Can I use a USB keyboard or mouse at the local port? .....	312
Is there an On-Screen Display (OSD) for local, at-the-rack access? .....	312
How do I select between servers while using the local port? .....	313
How do I ensure that only authorized users can access servers from the local port? .....	313
If I use the local port to change the name of a connected server, does this change propagate to remote access clients as well? Does it propagate to the optional CommandCenter appliance? .....	313
If I use KSX II's remote administration tools to change the name of a connected server, does that change propagate to the local port as well? .....	313
Sometimes I see "shadows" on the local port user interface. Why does that occur? .....	314
Power Control .....	314
Does the power supply used by KSX II automatically detect voltage settings? .....	314
What type of power control capabilities does KSX II offer? .....	314
Does KSX II support servers with multiple power supplies? What if each power supply is connected to a different power strip? .....	314
Does remote power control require any special server configuration? .....	314
What type of power strips does KSX II support? .....	315
Scalability .....	315
How do I connect multiple KSX II devices together into one solution? .....	315
Can I connect an existing analog KVM switch to KSX II? .....	315
Security .....	316
What kind of encryption does KSX II use? .....	316
Does KSX II support AES encryption as recommended by the US Government's NIST and FIPs standards? .....	316

Does KSX II allow encryption of video data? Or does it only encrypt keyboard and mouse data? .....316

How does KSX II integrate with external authentication servers such as Active Directory, RADIUS, or LDAP/S?.....316

How are usernames and passwords stored? .....316

Does KSX II support strong password? .....317

If the KSX II Encryption Mode is set to Auto, what level of encryption is achieved? .....317

Manageability.....317

    Can KSX II be remotely managed and configured via web browser? .....317

    Can I backup and restore KSX II's configuration? .....318

    What auditing or logging does KSX II offer? .....318

    Can KSX II integrate with Syslog? .....318

    Can KSX II integrate with SNMP? .....318

    Can KSX II's internal clock be synchronized with a timeserver? .....318

Miscellaneous.....318

    What is KSX II's default IP address? .....318

    What is KSX II's default username and password? .....319

    I changed and subsequently forgot KSX II's administrative password; can you retrieve it for me? (Share).....319

Troubleshooting.....319

    I am logged into the KSX II using Firefox, and I opened another Firefox browser. I am automatically logged into the same KSX II with the second Firefox browser. Is this right?319

    I am logged into the KSX II using Firefox and I attempt to log into another KSX II using another Firefox browser session from the same client. I am logged out of both KSX IIs; is this correct behavior? .....319





# Chapter 1 Introduction

## In This Chapter

Dominion KSX II Overview .....	2
Virtual Media .....	4
Product Photos.....	5
Product Features .....	6
Terminology.....	7
External Product Overview.....	9
Package Contents.....	12
User Guide.....	12

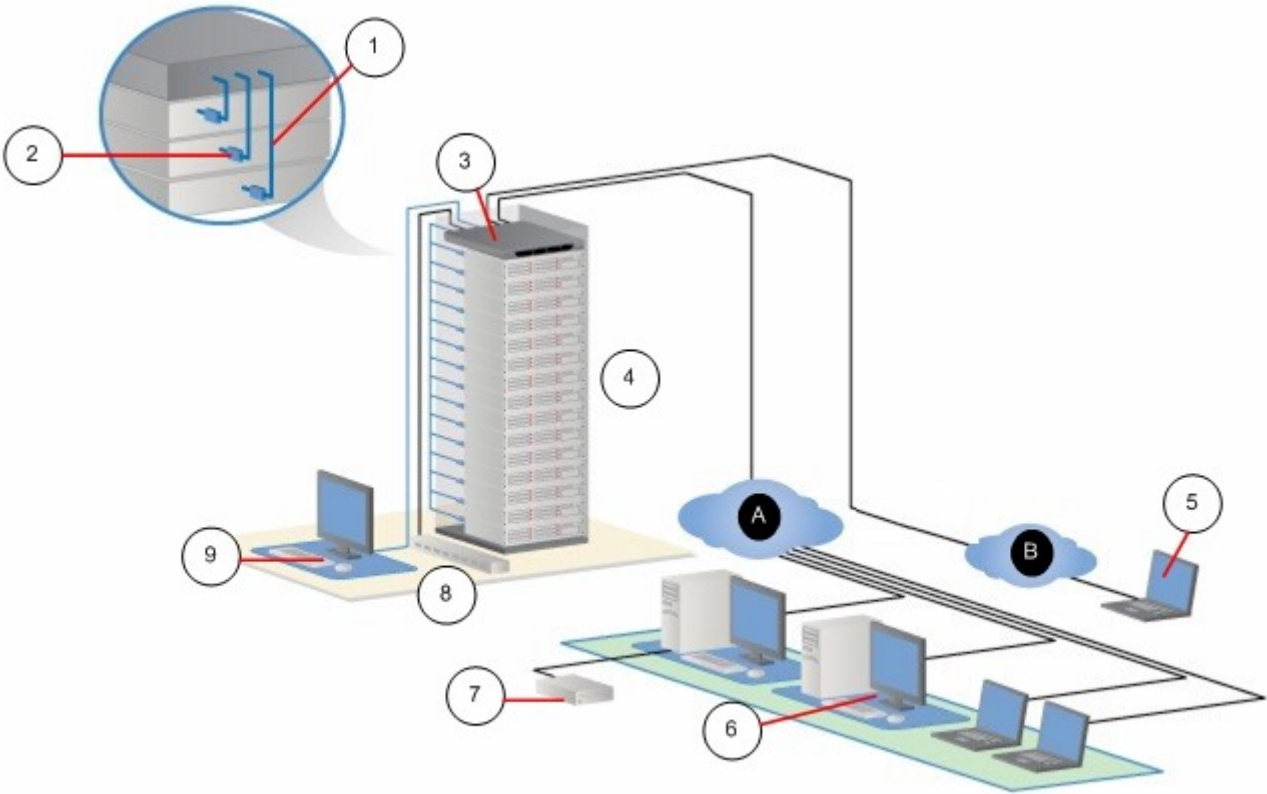
---

## **Dominion KSX II Overview**

The 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.

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



**Diagram Key**

- 1 Cat5 Cable
- 2 Computer Interface Module (CIM)
- 3 Dominion KSX II
- 4 Remote KVM and Serial Devices
- 5 Modem Access
- 6 Remote (Network) Access
- 7 Remote Virtual Media USB Drive(s)
- 8 Power Strip

## Virtual Media

### Diagram Key



Local Access



IP LAN/WAN



PSTN

---

## Virtual Media

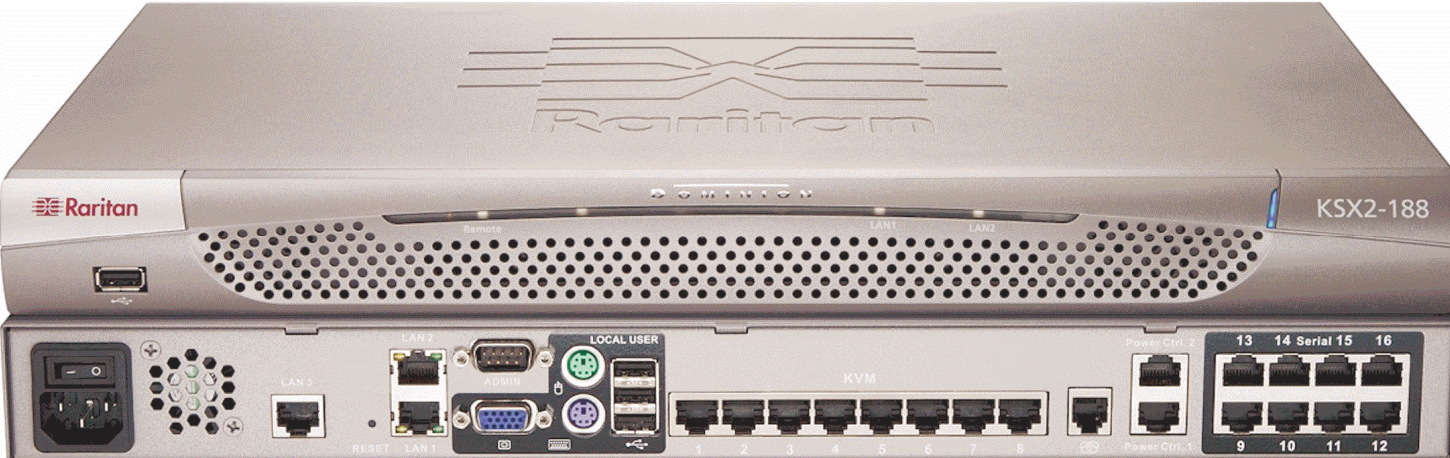
All KSX II models support virtual media. The benefits of virtual media - mounting of remote drives/media on the target server to support software installation, and diagnostics - are now available in all of the KSX II models.

Each KSX II comes equipped with virtual media to enable remote management tasks using the widest variety of CD, DVD, USB, internal and remote drives and images. Unlike other solutions, the KSX II supports virtual media access of hard drives and remotely mounted images for added flexibility and productivity.

Virtual media sessions are secured using 128-bit and 256-bit AES or RC4 encryption.

The new D2CIM-VUSB CIM (computer interface module) supports virtual media sessions to KVM target servers supporting the USB 2.0 interface. This new CIM also supports Absolute Mouse Synchronization as well as remote firmware update.

Product Photos



KSX II 144 and 188



CIM



Serial Adapter



---

## **Product Features**

---

### **Hardware**

- KVM and serial remote access over IP
- 1U (KSX II) 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
  - PS/2 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 accessed 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

---

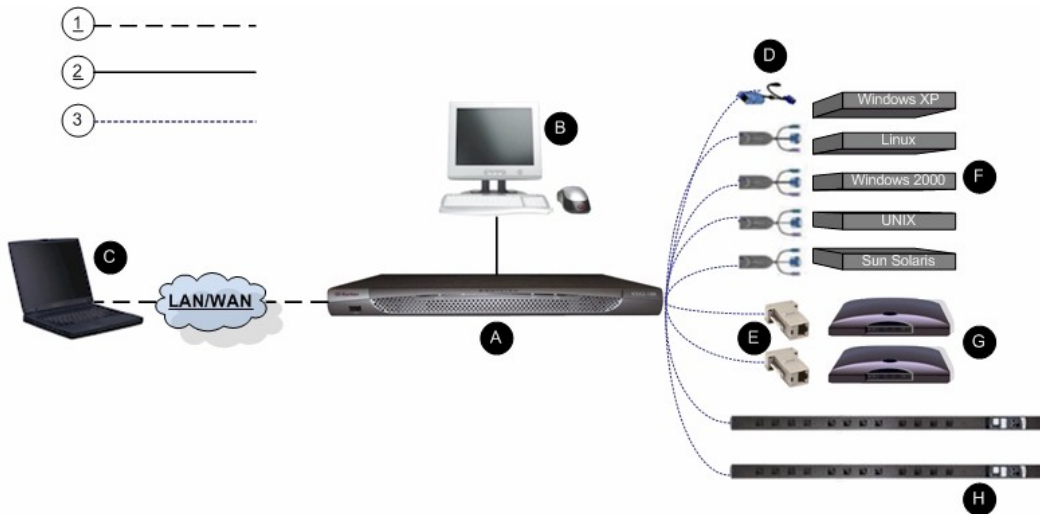
**Software**

- Virtual media with D2CIM-VUSB CIM
- Absolute Mouse Synchronization with D2CIM-VUSB CIM
- 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
- SNMP and Syslog management
- Power control associated directly with servers to prevent mistakes
- CC Unmanage feature to remove device from CC-SG control

---

**Terminology**

This manual uses the following terminology for the components of a typical KSX II configuration:



## Terminology

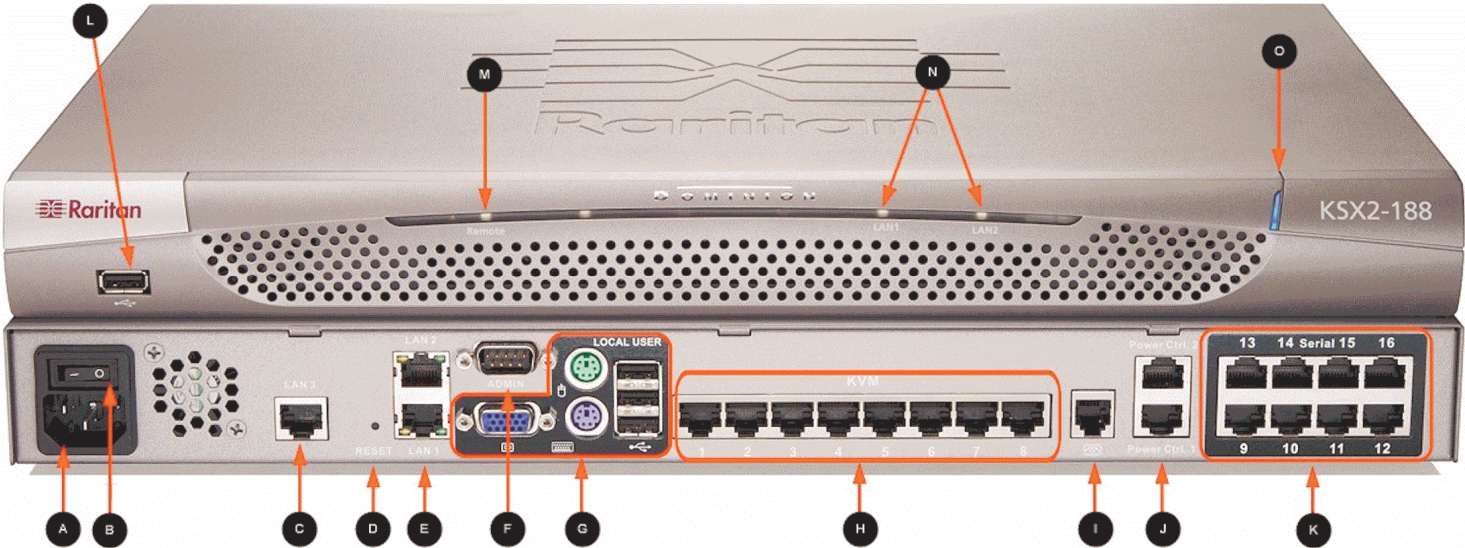
Diagram Key	
①	TCP/IP
②	KVM (Keyboard, Video, Mouse)
③	UTP Cable (Cat5/5e/6)
Ⓐ	KSX II
Ⓑ	<b>Local Access Console</b>  Local User - an optional user console (consisting of a keyboard, mouse, and multi-sync VGA monitor) attached directly to KSX II to control KVM target servers and serial targets locally (directly at the rack, not through the network).  Local Admin - 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.
Ⓒ	<b>Remote PC</b>  Networked computers used to access and control KVM target servers and serial targets connected to the KSX II. Refer to <i>Supported Operating Systems (Clients)</i> (on page 15) for a list of the Operating Systems supported by KSX II remotely.
Ⓓ	<b>CIMs</b>  Dongles that connect to each target server. Available for all of the supported Operating Systems. Refer to Supported CIMs for information about the CIMs supported by KSX II.
Ⓔ	<b>Serial Adapter</b>  Adapters that connect serial cables.



Diagram Key	
<b>F</b>	<b>Target Servers</b> KVM Target Servers - servers with video cards and user interfaces (e.g., Windows®, Linux®, Solaris™, etc.) accessed remotely via KSX II. Refer to Supported Operating Systems and CIMs (Target Servers) for a list of the supported Operating Systems and CIMs.  Serial Targets - Servers, routers, and switches that have a serial port accessed remotely via KSX II.
<b>G</b>	<b>Routers</b>
<b>H</b>	<b>Dominion PX Power Strip</b> Raritan power strips accessed remotely via the KSX II.



**External Product Overview**

The following diagram indicates the external components of the KSX II. Note that the the KSX II 144 will have 4 KVM ports and 4 serial ports as compared to the KSX II 188 used in the diagram, which has 8 KVM ports and 8 serial ports.



## External Product Overview

Item	Description	Item	Description
A	AC power cord plug See <i>Power Control</i> (on page 159) for additional information.	I	External modem port See <i>Modem Configuration</i> (on page 251) for additional information.
B	Power on/off switch	J	Power Ctrl. 1 and Power Ctrl. 2 See <i>Power Control</i> (on page 159) for additional information.
C	LAN 3 port Note: The LAN 3 port is reserved for future use.	K	Serial ports See <i>Step 4: Connect the Equipment</i> (on page 34) for additional information.
D	Reset button See <i>Reset Button</i> (on page 198) for additional information.	L	USB port
E	LAN1 and LAN2 ports See <i>Step 4: Connect the Equipment</i> (on page 34) for additional information.	M	Remote indicator light
F	Admin port See <i>Step 4: Connect the Equipment</i> (on page 34) for additional information.	N	LAN1 and LAN2 indicator lights

Item	Description
	Local port See <i>Step 4: Connect the Equipment</i> (on page 34) for additional information.
	KVM ports See <i>Step 4: Connect the Equipment</i> (on page 34) for additional information.

Item	Description
	Power indicator light

## Package Contents

---

### Package Contents

Each KSX II ships as a fully-configured stand-alone product in a standard 1U 19" rackmount chassis. Each KSX II unit ships with the following contents:

Amount Included	Item
1	Dominion KSX II Unit
1	Dominion KSX II Quick Setup Guide
1	Dominion KSX II User Manual CD-ROM
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 Note
1	Warranty Card
1	Phone Line Cable
1	Loopback Adapter

---

### User Guide

The KSX II User Guide provides information on the following:

- Installation, set up and configuration of the KSX II
- Accessing KVM target servers, serial targets, and power strips
- Using virtual media
- Managing users and security
- Maintaining and diagnosing the KSX II

---

## **Organization of Information**

The user guide is organized as follows:

- Chapter 1, Introduction. Overview, features, terminology, and package contents
- Chapter 2, Getting Started. Login information; default IP Address; supported operating systems, browsers, and CIMs
- Chapter 3, Installation and Configuration. Target server configuration; firewall settings; physical device connections; initial KSX II unit configuration; remote authentication; and users, groups, and access permissions
- Chapter 4, Connecting to the KSX II. User interfaces; starting the KSX II Remote Console; KSX II Favorites
- Chapter 5, Accessing Target Servers and Serial Targets. Access, control, and switching between KVM target servers
- Chapter 6, Virtual KVM Client. Target server control, mouse pointer synchronization, keyboard macros, and video settings
- Chapter 7, Virtual Media. Virtual media configuration and access
- Chapter 8, User Management. User and group management, passwords, group-based IP access control, and authentication settings
- Chapter 9, Device Management. Network settings, date/time, event management, power supply setup, port configuration, and power control
- Chapter 10, Security Settings. Security settings and IP access control
- Chapter 11, Maintenance. Audit log; device information; backup and restore; firmware and CIM upgrades; and reboot
- Chapter 12, Diagnostics. Network interface, network statistics, ping host, trace route to host, and KSX II diagnostics
- Chapter 13, KSX II Local Console. Starting the KSX II Local Console, accessing KVM target servers, and local port administration
- Chapter 14, CC Unmanage. Removing the KSX II from CC-SG control
- Appendix A, Specifications. Physical specifications; ports used; target server connection distance and video resolution; and network speed settings
- Appendix B, Updating the LDAP/LDAPS Schema. Update LDAP/LDAPS schema (for experienced users)
- Appendix C, Informational Notes. Important notes on KSX II usage

## User Guide

- Appendix D, FAQs. General questions, remote access, universal virtual media, Ethernet and IP networking, servers, installation, local port, power control, scalability, Computer Interface Modules (CIMs), security, manageability, miscellaneous, and troubleshooting

---

### Related Documentation

For more information about the Raritan Multi-Platform Client (MPC), refer to the Raritan Multi-Platform Client (MPC) User Guide.

For more information about the entire Raritan product line, refer to the Raritan User Manuals & Quick Setup Guides CD ROM or Raritan's website in the Support section.

# Chapter 2 Getting Started

## In This Chapter

Login Information.....	15
Default IP Address.....	15
Supported Operating Systems (Clients).....	15
Supported Browsers .....	16
Supported Operating Systems and CIMs (KVM Target Servers).....	16

---

## Login Information

- The default KSX II login user name is admin and the default password is raritan. This user has administrative privileges.
- Passwords are case sensitive and must be entered in the exact case combination in which they were created. For example, the default password raritan must be entered entirely in lowercase letters.
- The first time you start the KSX II you are required to change the default password.

---

*Tip: 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.*

---

---

## Default IP Address

KSX II ships with the default IP address of 192.168.0.192.

---

## Supported Operating Systems (Clients)

The following operating systems are supported on the Raritan Serial Console, Virtual KVM Client™, and Multi-Platform Client (MPC):

Client OS	Virtual Media (VM) Support on Client
Windows XP®	Yes
Windows 2000 SP4®	Yes
Windows Vista®	Yes

## Supported Browsers

Client OS	Virtual Media (VM) Support on Client
Red Hat® Linux 9.0	Yes; Locally held ISO image, Remote File Server mounting directly from KSX II
Red Hat Enterprise Workstation 3.0 and 4.0	Yes; Locally held ISO image, Remote File Server mounting directly from KSX II
SUSE Linux Professional 9.2 and 10	Yes; Locally held ISO image, Remote File Server mounting directly from KSX II
Fedora™ Core 5 and above	Yes; Locally held ISO image, Remote File Server mounting directly from KSX II
Mac®	No
Solaris®	No

---

## Supported Browsers

KSX II supports the following browsers:

- Internet Explorer 6 and 7
- Firefox 1.5 and 2.0
- Mozilla 1.7

---

## Supported Operating Systems and CIMs (KVM Target Servers)

In addition to the new D2CIMs, most Dominion CIMs are supported. The following table displays the supported target server operating systems, CIMs, virtual media, and mouse modes:

---

*Note: D2CIM-VUSB is not supported on Sun (Solaris) targets.*

---



Target Server	Supported CIMs		Mouse Modes			
	Dominion DCIMs	D2CIMs	VM	AM	IM	SM
Windows XP Windows 2000 Windows 2000 Server® Windows 2003 Server® Windows Vista	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓	✓	✓
Red Hat Linux 9.0  Red Hat Enterprise Workstation 3.0 and 4.0	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB (excluding Red Hat Enterprise Workstation 3.0)	✓			✓
SUSE Linux Professional 9.2 and 10	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Fedora Core 3® and above	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Mac OS	DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓		
All Solaris OSs supported in Dominion KSX II	DCIM-SUN DCIM-SUSB DCIM-USB G2					✓
IBM AIX®	DCIM-USB DCIM-USB G2 DCIM-PS2					✓

**Supported Operating Systems and CIMs (KVM Target Servers)**

Target Server	Supported CIMs		Mouse Modes			
	Dominion DCIMs	D2CIMs	VM	AM	IM	SM
HP UX®	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
Serial Devices						

Legend:

- VM: Virtual Media (D2CIM-VUSB only)
- AM: Absolute Mouse Synchronization (D2CIM-VUSB only)
- IM: Intelligent Mouse Mode
- SM: Standard Mouse Mode
- ✓: Supported

*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 KVM target servers; move the switch to S for Sun USB KVM target servers.*

*A new switch position takes effect only after the CIM is power-cycled. To power-cycle the CIM, remove the USB connector from the target server and plug it back in a few seconds later.*

# Chapter 3 Installation and Configuration

## In This Chapter

Overview .....	19
Step 1: Configure KVM Target Servers.....	19
Step 2 (Optional): Configure Keyboard Language .....	32
Step 3: Configure Network Firewall Settings.....	33
Step 4: Connect the Equipment.....	34
Step 5: KSX II Initial Configuration .....	38

---

## Overview

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

➤ **To install and configure KSX II:**

1. Configure the KVM target servers.
2. (Optional) Configure the keyboard language.
3. Configure the network firewall settings.
4. Connect the equipment.
5. Configure the KSX II unit.

---

## Step 1: Configure KVM Target Servers

KVM target servers are the computers that will be accessed and controlled via the KSX II. Before installing KSX II, configure all KVM target servers to ensure optimum performance. This configuration applies only to KVM target servers, not to the client workstations (remote PCs) used to access KSX II remotely. Refer to Chapter 1: Introduction, Terminology for additional information.

➤ **To configure the KVM target servers:**

- Check the video resolution.
- Check the desktop background.
- Adjust the mouse settings.
- Perform OS-specific mouse and video configuration.

## Step 1: Configure KVM Target Servers

---

### Supported Video Resolutions

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

Video resolution and cable length are important factors in the ability to obtain mouse synchronization. Refer to *Target Server Connection Distance and Video Resolution* (on page 270) for more information. KSX II supports these resolutions:

640x350 @70 Hz	720x400 @85 Hz	1024x768 @90 Hz
640x350 @85 Hz	800x600 @56 Hz	1024x768 @100 Hz
640x400 @56 Hz	800x600 @60 Hz	1152x864 @60 Hz
640x400 @84 Hz	800x600 @70 Hz	1152x864 @70 Hz
640x400 @85 Hz	800x600 @72 Hz	1152x864 @75 Hz
640x480 @60 Hz	800x600 @75 Hz	1152x864 @85 Hz
640x480 @66.6 Hz	800x600 @85 Hz	1152x870 @75.1 Hz
640x480 @72 Hz	800x600 @90 Hz	1152x900 @66 Hz
640x480 @75 Hz	800x600 @100 Hz	1152x900 @76 Hz
640x480 @85 Hz	832x624 @75.1 Hz	1280x960 @60 Hz
640x480 @90 Hz	1024x768 @60 Hz	1280x960 @85 Hz
640x480 @100 Hz	1024x768 @70 Hz	1280x1024 @60 Hz
640x480 @120 Hz	1024x768 @72 Hz	1280x1024 @75 Hz
720x400 @70 Hz	1024x768 @75 Hz	1280x1024 @85 Hz
720x400 @84 Hz	1024x768 @85 Hz	1600x1200 @60 Hz

---

*Note: Composite Sync and Sync-on-Green video require an additional adapter.*

---

### Desktop Background

For optimal bandwidth efficiency and video performance, KVM target servers running graphical user interfaces such as Windows, Linux, X-Windows, Solaris, and KDE require configuration. The desktop background need not be completely solid; but desktop backgrounds featuring photos or complex gradients might degrade performance.

---

## **Mouse Settings**

The KSX II operates in several mouse modes:

- *Absolute Mouse Synchronization* (see "Absolute" on page 101) (D2CIM-VUSB only)
- *Intelligent Mouse Mode* (see "Intelligent" on page 101) (do not use an animated mouse)
- *Standard Mouse Mode* (see "Standard" on page 100)

For both the Standard and Intelligent mouse modes, mouse parameters must be set to specific values, which are described later in this manual. Mouse parameters do not have to be altered for Absolute Mouse Synchronization; D2CIM-VUSB is required for this mode. Mouse configurations will vary on different target operating systems; consult your OS documentation for additional detail.

Intelligent mouse mode generally works well on most Windows platforms. Intelligent mouse mode may produce unpredictable results when active desktop is set on the target. For additional information on Intelligent Mouse mode, refer to the Raritan Multi-Platform Client (MPC) User Guide (Appendix B: Conditions for Intelligent Mouse Synchronization) available on Raritan's Website <http://www.raritan.com/support/productdocumentation>, or on the Raritan User Manuals & Quick Setup Guides CD ROM included with your KSX II shipment.

---

## **Operating System Mouse and Video Settings**

This section provides video mode and mouse information specific to the Operating System in use on the target server.

---

### **Windows XP / Windows 2003 Settings**

➤ ***To configure KVM target servers running Microsoft Windows XP/2003:***

1. Configure the mouse settings:
  - a. Choose Start > Control Panel > Mouse.
  - b. Click the Pointer Options tab.
  - c. In the Motion group:

## Step 1: Configure KVM Target Servers

- Set the mouse motion speed setting exactly to the middle speed.
  - Disable the Enhanced pointer precision option.
  - Click OK.
2. Disable transition effects:
    - a. Select the Display option from Control Panel.
    - b. Click the Appearance tab.
    - c. Click the Effects button.
    - d. Deselect the Use the following transition effect for menus and tooltips option.
    - e. Click OK.
    - f. Close the Control Panel.

---

*Note: For KVM target servers running Windows 2000 or XP, you may wish to create a user name that will be used only for remote connections through KSX II. This will enable you to keep the target server's slow mouse pointer motion/acceleration settings exclusive to the KSX II connection.*

*Windows XP and 2000 login screens revert to pre-set mouse parameters that differ from those suggested for optimal KSX II performance. As a result, mouse synchronization may not be optimal for these screens. WARNING! Proceed only if you are comfortable adjusting the registry on Windows KVM target servers. You can obtain better KSX II mouse synchronization at login screens by using the Windows registry editor to change the following settings (HKEY\_CURRENT\_USER\Control Panel\Mouse): MouseSpeed = 0; MouseThreshold 1= 0; MouseThreshold 2 = 0.*

---

## Windows 2000 Settings

- **To configure KVM target servers running Microsoft Windows 2000:**
1. Configure the mouse settings:
    - a. Choose Start > Control Panel > Mouse.
    - b. Click the Motion tab.

- Set the acceleration to None.
  - Set the mouse motion speed setting exactly to the middle speed.
  - Click OK.
2. Disable transition effects:
    - a. Select the Display option from Control Panel.
    - b. Click the Effects tab.
    - c. Deselect the Use the following transition effect for menus and tooltips option.
    - d. Click OK.
    - e. Close the Control Panel.

---

## **Windows Vista**

➤ ***To configure KVM target servers running Microsoft Windows Vista:***

1. Configure the mouse settings:
  - a. Choose Start > Settings > Control Panel > Mouse.
  - b. Click the Pointer Options tab.
  - c. In the Motion group:
    - Set the mouse motion speed setting exactly to the middle speed.
    - Disable the Enhanced pointer precision option.
    - Click OK.
2. Disable animation and fade effects:
  - a. Select the System option from Control Panel.
  - b. Select Advanced system settings. The System Properties dialog opens.
  - c. Click the Advanced tab.
  - d. Click the Settings button in the Performance group. The Performance Options dialog opens.
  - e. Under Custom options, deselect the following checkboxes:
    - Animation options:
      - Animate controls and elements inside

## Step 1: Configure KVM Target Servers

- Animate windows when minimizing and maximizing
  - Fade options:
    - Fade or slide menus into view
    - Fade or slide ToolTips into view
    - Fade out menu items after clicking
- a. Click OK.
  - b. Close the Control Panel.

---

### Linux Settings (Red Hat 9)

---

*Note: The following settings are optimized for standard mouse mode only.*

---

➤ **To configure KVM target servers running Linux (graphical user interface):**

1. Configure the mouse settings:
  - a. Choose Main Menu > Preferences > Mouse. The Mouse Preferences dialog opens.
  - b. Click the Motion tab.
  - c. Within the Speed group, set the Acceleration slider to the exact center.
  - d. Within the Speed group, set the Sensitivity towards low.
  - e. Within the Drag & Drop group, set the Threshold towards small.
  - f. Close the Mouse Preferences dialog.

---

Note: If these steps do not work, issue the `xset mouse 1 1` command as described in the Linux command line instructions.

---

2. Configure the screen resolution:
  - a. Choose Main Menu > System Settings > Display. The Display Settings dialog opens.
  - b. From the Display tab, select a Resolution supported by KSX II.
  - c. From the Advanced tab, verify that the Refresh Rate is supported by KSX II.



---

*Note: Once connected to the target server, in many Linux graphical environments, the <CTRL> <ALT> <+> command will change the video resolution, scrolling through all available resolutions that remain enabled in the XF86Config file.*

---

➤ **To configure KVM target servers running Linux (command line):**

1. Set the mouse acceleration to exactly 1 and set the threshold to exactly 1. Enter this command: `xset mouse 1 1`. This should be set for execution upon login.
2. Ensure that each target server running Linux is using a resolution supported by KSX II at a standard VESA resolution and refresh rate.
3. Each Linux target server should also be set so the blanking times are within +/- 40% of VESA standard values:
  - a. Go to the Xfree86 Configuration file XF86Config.
  - b. Using a text editor, disable all non-KSX II supported resolutions.
  - c. Disable the virtual desktop feature (not supported by KSX II).
  - d. Check blanking times (+/- 40% of VESA standard).
  - e. Restart computer.

---

*Note: If you change video resolution, you must logout of the target server and log back in for the video settings to take effect.*

---

**Note for Red Hat 9 KVM Target Servers**

If you are running Red Hat 9 on the target server using a USB CIM, and are experiencing problems with the keyboard and/or mouse, there is an additional configuration setting you can try.

---

*Tip: You might have to perform these steps even after a fresh OS installation.*

---

➤ **To configure Red Hat 9 servers using USB CIMs:**

1. Locate the configuration file (usually `/etc/modules.conf`) in your system.
2. Using the editor of your choice, make sure that the alias `usb-controller` line in the `modules.conf` file is as follows:

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

---

*Note: If there is another line using `usb-uhci` in the `/etc/modules.conf` file, it needs to be removed or commented out.*

---

## Step 1: Configure KVM Target Servers

3. Save the file.
4. Reboot the system in order for the changes to take effect.

---

### Linux Settings (Red Hat 4)

---

*Note: The following settings are optimized for standard mouse mode only.*

---

➤ **To configure KVM target servers running Linux (graphical user interface):**

1. Configure the mouse settings:
  - a. Choose Main Menu > Preferences > Mouse. The Mouse Preferences dialog opens.
  - b. Open the Motion tab.
  - c. Within the Speed group, set the Acceleration slider to the exact center.
  - d. Within the Speed group, set the Sensitivity towards low.
  - e. Within the Drag & Drop group, set the Threshold towards small.
  - f. Close the Mouse Preferences dialog.

---

*Note: If these steps do not work, issue the `xset mouse 1 1` command as described in the Linux command line instructions.*

---

2. Configure the screen resolution:
  - a. Choose Main Menu > System Settings > Display. The Display Settings dialog opens.
  - b. From the Settings tab, select a Resolution supported by KSX II.
  - c. Click OK.

---

*Note: If you change video resolution, you must logout of the target server and log back in for the video settings to take effect.*

---

---

### SUSE Linux 10.1 Settings

---

*Note: Do not attempt to synchronize the mouse at the SUSE login prompt. You must be connected to the target server to synchronize the mouse cursors.*

---

➤ **To configure the mouse settings:**

1. Choose Desktop > Control Center. The Desktop Preferences dialog opens.

2. Click Mouse. The Mouse Preferences dialog opens.
3. Open the Motion tab.
4. Within the Speed group, set the Acceleration slider to the exact center position.
5. Within the Speed group, set the Sensitivity slider to low.
6. Within the Drag & Drop group, set the Threshold slider to small.
7. Click Close.

➤ **To configure the video:**

1. Choose Desktop Preferences > Graphics Card and Monitor. The Card and Monitor Properties dialog opens.
2. Verify that a Resolution and Refresh Rate is in use that is supported by KSX II. Refer to Supported Video Resolutions for more information.

---

Note: If you change video resolution, you must log out of the target server and log back in for the video settings to take effect.

---

---

### Make Linux Settings Permanent

---

*Note: These steps may vary slightly depending on the specific version of Linux in use.*

---

➤ **To make your settings permanent in Linux (prompt):**

1. Choose Main Menu > Preferences > More Preferences > Sessions. The Sessions dialog opens.
2. Click the Session Options tab.
3. Select the Prompt on log out checkbox and click OK. This option prompts you to save your current session when you log out.
4. Upon logging out, select the Save current setup option from the dialog presented.
5. Click OK.

---

*Tip: If you do not want to be prompted upon log out, follow these procedures instead.*

---

➤ **To make your settings permanent in Linux (no prompt):**

1. Choose Main Menu > Preferences > More Preferences > Sessions. The Session dialog opens.

## Step 1: Configure KVM Target Servers

2. Click the Session Options tab.
3. Deselect the Prompt on the logout checkbox.
4. Select the Automatically save changes to the session checkbox and click **OK**. This option automatically saves your current session when you log out.

---

### Make UNIX Settings Permanent

---

*Note: These steps may vary slightly depending on the type of UNIX® (e.g., Solaris, IBM AIX) and the specific version in use.*

---

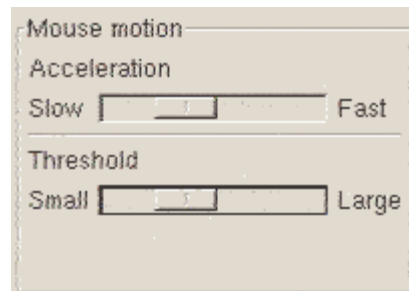
1. Choose Style Manager > Startup. The Style Manager - Startup dialog opens.
2. Select the Logout Confirmation dialog option of On. This option prompts you to save your current session when you logout.

---

### Sun Solaris Settings

➤ **To configure KVM target servers running Sun Solaris:**

1. Set the mouse acceleration value to exactly 1 and the threshold to exactly 1. This can be performed:
  - From the graphical user interface:



- With the command line:  

```
xset mouse a t
```

(where "a" is the acceleration and "t" is the threshold.)
2. All KVM target servers must be configured to one of the display resolutions supported by KSX II. The most popular supported resolutions for Sun machines are:

Display Resolution	Vertical Refresh Rate	Aspect Ratio
1600 x 1200	75 Hz	4:3
1280 x 1024	60,75,85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60,70,75,85 Hz	4:3
800 x 600	56,60,72,75,85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60,72,75,85 Hz	4:3

3. KVM target servers running the Solaris operating system must output VGA video (H-and-V sync, not composite sync).

➤ **To change your Sun video card output from composite sync to the non-default VGA output:**

1. Issue the Stop+A command to drop to bootprom mode.
2. Issue the following command to change the output resolution:  
`setenv output-device screen:r1024x768x70`
3. Issue the "boot" command to reboot the server.

You can also contact your Raritan representative to purchase a video output adapter:

If you Have:	Use this Video Output Adapter:
Sun 13W3 with composite sync output	APSSUN II Guardian converter
Sun HD15 with composite sync output	1396C converter to convert from HD15 to 13W3 and an APSSUN II Guardian converter to support composite sync
Sun HD15 with separate sync output	APKMSUN Guardian converter

## Step 1: Configure KVM Target Servers

---

*Note: Some of the standard Sun background screens may not center precisely on certain Sun servers, with dark borders. Use another background or place a light colored icon in the upper left hand corner.*

---

### Mouse Settings

➤ **To configure the mouse settings (Sun Solaris 10.1):**

1. Choose Launcher. Application Manager - Desktop Controls opens.
2. Choose Mouse Style Manager. The Style Manager - Mouse dialog opens.
3. Set the Acceleration slider to 1.0.
4. Set the Threshold slider to 1.0.
5. Click OK.

### Accessing the Command Line

1. Right click.
2. Choose Tools > Terminal. A terminal window opens. (It is best to be at the root to issue commands.)

### Video Settings (POST)

Sun systems have two different resolution settings: a POST resolution and a GUI resolution. Please Note that 1024x768x75 is used as an example here; substitute the resolution and refresh rate you are using. Run these commands from the command line.

➤ **To check current POST resolution:**

- Run the following command as root: # eeprom output-device

➤ **To change POST resolution:**

1. # eeprom output-device=screen:r1024x768x75
2. Logout or restart computer.

**Video Settings (GUI)**

The GUI resolution can be checked and set using different commands depending on the video card in use. Please Note that 1024x768x75 is used as an example here; substitute the resolution and refresh rate you are using. Run these commands from the command line.

The following table is organized by card:

Card	To Check Resolution:	To Change Resolution:
32-bit	# /usr/sbin/pgxconfig -prconf	<ol style="list-style-type: none"> <li># /usr/sbin/pgxconfig -res 1024x768x75</li> <li>Logout or restart computer.</li> </ol>
64-bit	# /usr/sbin/m64config -prconf	<ol style="list-style-type: none"> <li># /usr/sbin/m64config -res 1024x768x75</li> <li>Logout or restart computer.</li> </ol>
32-bit and 64-bit	# /usr/sbin/fbconfig -prconf	<ol style="list-style-type: none"> <li># /usr/sbin/fbconfig -res 1024x768x75</li> <li>Logout or restart computer.</li> </ol>

---

**IBM AIX 5.3 Settings**

Follow these steps in this section to configure KVM target servers running IBM AIX 5.3.

➤ **To configure the mouse:**

1. Go to Launcher.
2. Choose Style Manager.
3. Click Mouse. The Style Manager - Mouse dialog opens.
4. Use the sliders to set the Mouse acceleration to 1.0 and Threshold to 1.0.
5. Click OK.

➤ **To configure the video:**

1. From the Launcher, select Application Manager.
2. Select System\_Admin.
3. Choose Smit > Devices > Graphic Displays > Select the Display Resolution and Refresh Rate.

## Step 2 (Optional): Configure Keyboard Language

4. Select the video card in use.
5. Click List. A list of display modes is presented.
6. Select a resolution and refresh rate supported by the KSX II. Please refer to Supported Video Resolutions for more information.

---

*Note: If you change video resolution, you must logout of the target server and log back in for the video settings to take effect.*

---

### Apple Macintosh Settings

For KVM target servers running an Apple Macintosh operating system, the preferred method is to use the D2CIM-VUSB and Absolute Mouse Synchronization.

---

*Note: Enable the Absolute Mouse Scaling for the MAC server option on the Port page.*

---

---

## Step 2 (Optional): Configure Keyboard Language

---

*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 has to be configured for the appropriate language. In addition, the keyboard language for the client machine and the KVM target servers has to match.

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

---

### Change the Keyboard Layout Code (Sun Targets)

Use this procedure if you are using a DCIM-SUSB and would like the keyboard layout changed 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 and press the left CTRL key and the DEL key on your keyboard. The Caps Lock LED 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).



4. Press Enter.
5. Shut down the unit and power ON once again. The DCIM-SUSB performs a reset (power cycle).
6. Using MPC, type something to verify that the characters are correct.

---

### Step 3: Configure Network Firewall Settings

To access KSX II through a network firewall, your firewall must allow communication on TCP Port 5000 or another port that you designate. Refer to Network Settings for additional information about designating another discovery port.

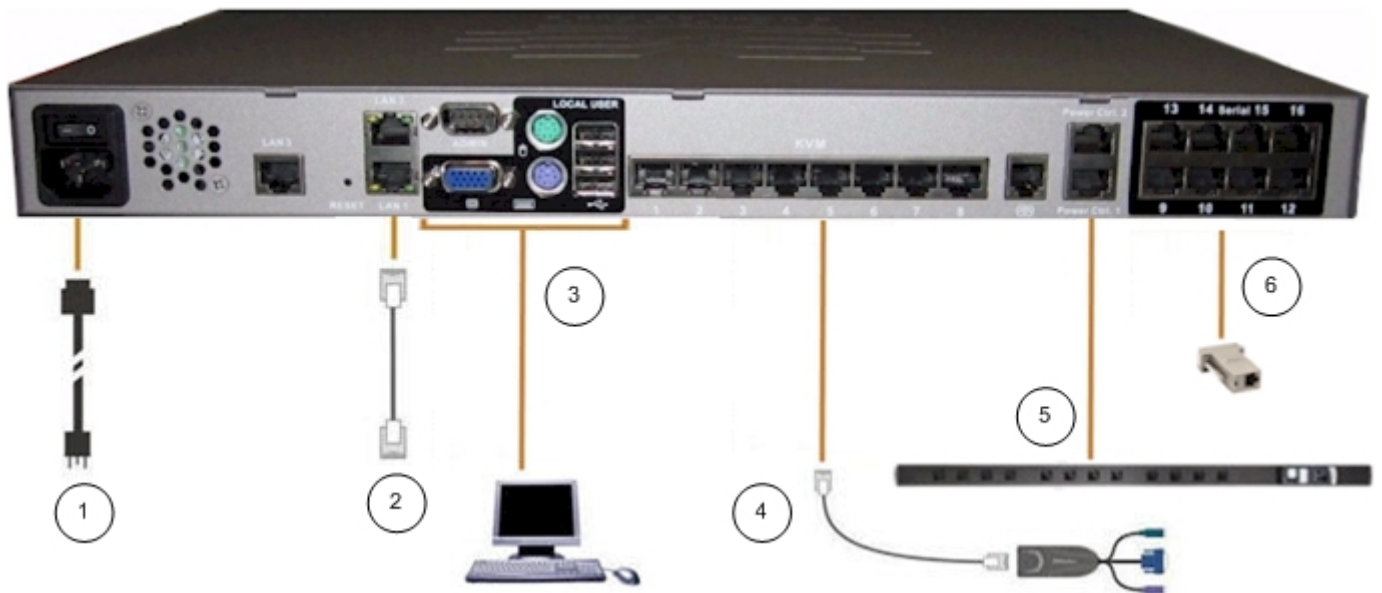
<b>To take advantage of the KSX II:</b>	<b>The firewall must allow inbound communication on:</b>
Web-access capabilities	Port 443 - standard TCP port for HTTPS communication
Automatic redirection of HTTP requests to HTTPS (i.e., so users can type the more common "http://xxx.xxx.xxx.xxx" instead of "https://xxx.xxx.xxx.xxx")	Port 80 - standard TCP port for HTTP communication

## Step 4: Connect the Equipment

---

### Step 4: Connect the Equipment

Connect the KSX II to the power supply, network, local PC, KVM target servers, and serial targets. The numbers in the diagram correspond to the sections describing the connection.



---

#### 1. 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.

---

#### 2. Network Ports

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.

➤ **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 screen (refer to Network Settings, LAN Interface Settings for more information).

---

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

---

### 3. 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, mouse, and keyboard to the respective Local User ports (using either a PS/2 or USB keyboard and mouse).

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.

---

### 4. KVM Target Server Ports

The KSX II uses standard UTP cabling (Cat5/5e/6) to connect to each target server. Refer to *Appendix A: Specifications* (see "Specifications" on page 265) for additional information.

#### ➤ **To connect a KVM target server to the KSX II:**

1. Use the appropriate Computer Interface Module (CIM). Refer to Supported Operating Systems and CIMs for more information about the CIMs to use with each operating system.
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.

## Step 4: Connect the Equipment

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 unit.

---

*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.*

*A new switch position takes effect only after the CIM is power-cycled. To power-cycle the CIM, remove the USB connector from the target server and plug it back in a few seconds later.*

---

## 5. 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 power strip outlet.
4. Connect the power strip to an AC power source.
5. Power ON the KSX II unit.

---

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

---

## 6. 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.

<b>Vendor</b>	<b>Device</b>	<b>Console Connector</b>	<b>Serial Connection</b>
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 CAT 5 cable
Silicon Graphics	Origin		
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 following link to obtain a list of commonly used cables and adapters <http://www.raritan.com/support>

---

## **Step 5: KSX II Initial Configuration**

The first time you power up the KSX II unit, there is some initial configuration that you need to perform through the KSX II Local Console:

- Change the default password.
- Assign the IP Address.
- Name the KVM target servers and serial targets.

---

### **Changing the Default Password**

The KSX II ships with a default password. The first time you start the KSX II you are required to change that password.

➤ **To change the default password:**

1. Power ON the KSX II using the power switch(es) at the back of the unit. Wait for the KSX II unit to boot. (A beep signals that the boot is complete.)
2. Once the unit has booted, the KSX II Local Console is visible on the monitor attached to the KSX II local port. Type the default username (admin) and password (raritan) and click Login. The Change Password screen is displayed.
3. Type your old password (raritan) in the Old Password field.
4. 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 the special characters identified in the table following these steps.
5. Click Apply.
6. You will receive confirmation that the password was successfully changed. Click OK. The Port Access page is displayed.

---

*Note: The default password can also be changed from the Raritan Multi-Platform Client (MPC). For more information, refer to the Raritan Multi-Platform Client (MPC) User Guide.*

---

### Assign an IP Address

These procedures describe how to assign an IP Address using the Network Settings page. For complete information about all of the fields and the operation of this page, refer to Network Settings.

1. From the KSX II Local Console, select Device Settings > Network Settings. The Network Settings page opens.

Home > Device Settings > Network Settings

**Network Basic Settings**

Device Name \*  
PM\_KSX2

IP auto configuration  
None

Preferred host name (DHCP only)  
[ ]

IP address  
192.168.59.248

Subnet mask  
255.255.255.0

Gateway IP address  
192.168.59.126

Primary DNS server IP address  
[ ]

Secondary DNS server IP address  
[ ]

**LAN Interface Settings**

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

Current LAN interface parameters:  
autonegotiation on, 100 Mbps, full duplex, link ok

**LAN Interface Speed & Duplex**  
Autodetect

Enable Automatic Failover

Ping Interval (seconds) \*  
30

Timeout (seconds) \*  
60

Bandwidth Limit  
No Limit

[Set System ACL](#)

2. Specify a meaningful Device Name for your KSX II unit; up to 16 alphanumeric characters, special characters, and no spaces.
3. Select the IP auto configuration from the drop-down list:
  - None (Static IP). This option requires that 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.
  - DHCP. With this option, network parameters are assigned by the DHCP server.
4. If you specify an IP configuration of None, type the TCP/IP parameters for your KSX II unit: IP address, Subnet mask, Gateway IP address, Primary DNS server IP address, and (optional) Secondary DNS server IP address.
5. When finished, click OK.

## Step 5: KSX II Initial Configuration

Your KSX II unit is now network accessible.

---

*Note: In some environments, the LAN Interface Speed & Duplex setting default of Autodetect (auto-negotiation) does not properly set the network parameters, resulting in network issues. In these instances, setting the KSX II LAN Interface Speed & Duplex field to 100 Mbps/Full Duplex (or whatever option is appropriate to your network) addresses the issue. Refer to the Network Settings page for more information.*

---

### Configure Direct Port Access

➤ **To configure direct port access:**

1. Choose Device Settings > Device Services. The Device Service Settings page appears.
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, access 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, access 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, access to the target can be done by using "ssh -l <login> <KSX II device IP address> -p 7888".



### Chapter 3: Installation and Configuration

Home > Device Settings > Device Services

Services		Direct Port Access				
Discovery Port *	5000	Port Number	Port Name	IP Address	SSH TCP Port	Telnet TCP Port
<input type="checkbox"/> Enable TELNET Access		9	Cisco 2501		2209	
TELNET Port	23	10	SP-2			
<input checked="" type="checkbox"/> Enable SSH Access		11	Serial Port 3			
SSH Port	22	12	Serial Port 4			
<input type="checkbox"/> Enable Serial Console Access		13	SP - 5			
Baud Rate:	9600	14	Serial Port 6			
		15	Serial Port 7			
		16	Serial Port 8			

OK    Reset To Defaults    Cancel

3. Click OK to save this information.
4. For information on

## Step 5: KSX II Initial Configuration

---

### Configure KVM and Serial Ports

Port configuration allows Administrators to define KVM and serial port settings in order to communicate with remote target devices. This section contains information on the following, which are all a part of the port configuration process:

- Naming KVM targets and serial targets (including valid special characters that can be used)
- Creating power associations for KVM and serial targets
- Defining KVM target server settings
- Defining serial port settings

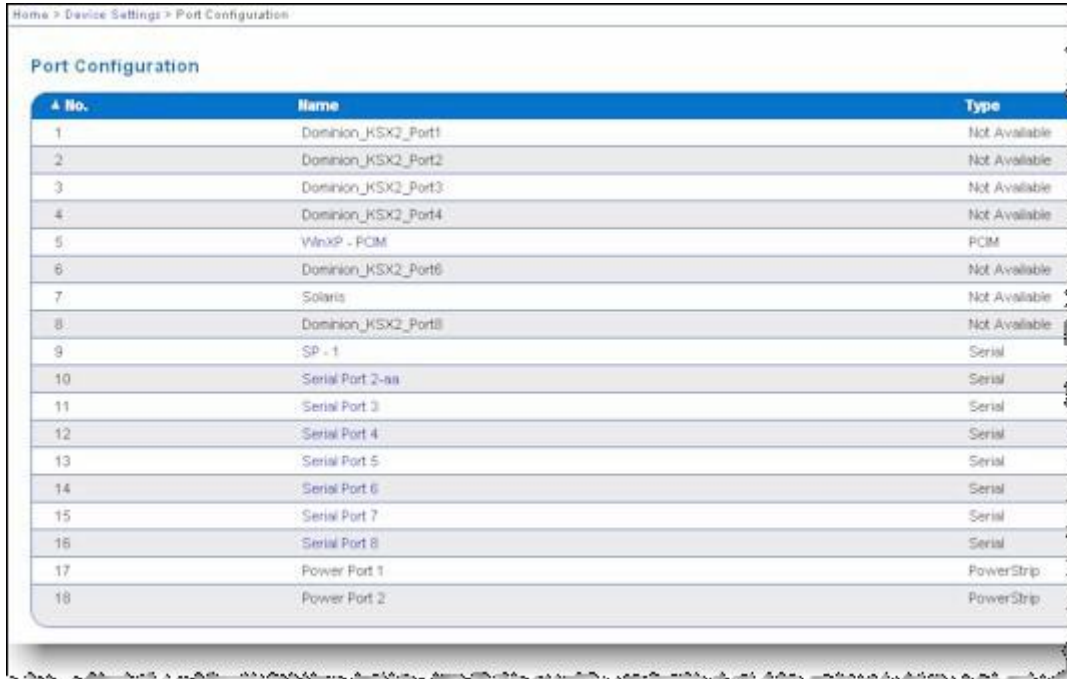
### Name KVM and Serial Targets

Note that the KVM and serial target names are defined on different Port pages (either a KVM or serial Port page) but the steps involved are the same for both. The only variation is selecting a KVM target or serial target from the Port Configuration page to access the appropriate Port page.

➤ **To name KVM target servers and serial targets:**

1. Connect all of the KVM target servers and serial targets if you have not already done so (as described in *Step 4: Connect the Equipment* (on page 34)).

- Using the KSX II Local Console, select Device Settings > Port Configuration. The Port Configuration page opens.



- Click the Port Name of the KVM target server or serial target you want to rename. The Port page opens. The fields on the Port page will vary for KVM and serial targets.
- Assign a name to identify the server or serial target connected to that port. The name can be up to 32 characters; alphanumeric and special characters are allowed.
- Click OK.

**Valid Special Characters for Target Names**

Character	Description	Character	Description
!	Exclamation point	:	Colon
"	Double quote	;	Semi-colon
#	Pound sign	=	Equal sign
\$	Dollar sign	>	Greater than sign
%	Percent sign	?	Question mark
&	Ampersand	@	At sign

## Step 5: KSX II Initial Configuration

Character	Description	Character	Description
'	Single quote	[	Left bracket
(	Left parenthesis	\	Backward slash
)	Right parenthesis	]	Right bracket
*	Asterisk	^	Caret
+	Plus sign	_	Underscore
,	Comma	`	Grave accent
-	Dash	{	Left brace
.	Period		Pipe sign
/	Forward slash	}	Right brace
<	Less than sign	~	Tilde

### **Associate KVM and Serial Target Servers to Outlets**

A server can have up to four power plugs and you can associate a different power strip with each. From 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 power strip outlets to target servers):**

---

*Note: When a power strip 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 power strip from the Power Strip Name drop-down list.
2. For that power strip, 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 cancel without saving changes:**

1. Click the Cancel button.

➤ **To remove a power strip association:**

1. Select the appropriate power strip from the Power Strip Name drop-down list.
2. For that power strip, select the appropriate outlet from the Outlet Name drop-down list.
3. From the Outlet Name drop-down list, select None.
4. Click OK. That power strip/outlet association is removed. A confirmation message is displayed.

Alternately, you can select the power strip from the Power Strip Name drop-down and then assign it a different outlet from the Outlet Name drop-down. Click OK to apply the changes. This will remove the power strips current association and associate it with the newly selected outlet. This method is not recommended by Raritan.

**Configure KVM Target Server Settings**

➤ **To configure a KVM**

The screenshot shows a web-based configuration interface for a KVM port. At the top, a breadcrumb trail reads 'Home > Device Settings > Port Configuration > Port'. Below this, a blue header bar identifies the section as 'Port 1'. The 'Type' is listed as 'VM' and the 'Name' is 'Win Target1'. The 'Power Association' section contains two columns of dropdown menus: 'Power Strip Name' and 'Outlet Name', each with four entries, all currently set to 'None'. The 'Target Server Settings' section includes two unchecked checkboxes: 'Absolute mouse scaling for MAC server' and 'Use Full Speed for Virtual Media CIM - Useful for BIOS that cannot handle High Speed USB devices'. At the bottom, there are 'OK' and 'Cancel' buttons.

**port:**

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.
2. Click a KVM port to configure. The Port page opens.

## Step 5: KSX II Initial Configuration

3. Enter or edit the name for the port and make or remove power associations as needed. Click OK to apply the settings.
4. If you are using VM-CIMs, the following options will be available:
  - a. Check the Absolute mouse scaling for MAC server option if you are using the D2CIM-VUSB CIM for a Mac target server.
  - b. Check the Use Full Speed for Virtual Media CIM option for use the high speed BIOS devices.

---

Note: For SUSE 9.2 KVM target servers, please enable (check) the Use Full Speed for Virtual Media CIM option for those target server ports. SUSE 9.2 does not work with the Virtual Media CIM when high speed is negotiated.

---

- c. Click OK.

### Configure Serial Port Settings

#### ➤ **To configure a serial port:**

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.
2. Click a serial port to configure. The Port page opens. The Application field is read-only.
3. Select the terminal emulation type from the Emulation drop-down menu. The choices are:

- VT100

---

Note: VT100 is only supported by the Local Console port. Other options may not be recognized.

---

- VT220
  - VT320
  - ANSI
4. Make sure the port values match the target system's serial port configuration:
    - a. Select the Baud Rate from the Baud Rate drop-down menu. The choices are:

- 9600
  - 19200
  - 28200
  - 38400
  - 57600
  - 115200
- b. Select the Parity Bits from the Parity Bits drop-down menu:
- None/8
  - Odd/7
  - Even/7
- c. Select the Flow Control from the Flow Control drop-down menu.
- Hardware
  - X on/ X off

---

Note: From a user perspective, data loss may be observed when SW flow control is used at very high data rates. If so, you should switch to HW flow control (on both KSX and the target server).

---

5. If you plan to use Direct Port Access (DPA), you must enter one of the following:
- The DPA IP Address.
  - The port number, such as 7700, in the DPA SSH TCP Port field.
    - The port number, such as 8800, in the DPA Telnet TCP Port field.
6. The escape mode is set to the default of Control.
7. Type the Escape Character. The default is ] (closed bracket ).
8. Type up to 10 commands in the Exit Command field. This is the command that will be sent to your system when a port disconnection occurs, for example, logout. For example, Command1;Command2 or Command1#<timeinterval>;Command#2<timeinterval>;...
9. Click OK.

## Step 5: KSX II Initial Configuration

---

Note: See *Port Keywords* (on page 165) for information on the Port Keywords section of the serials Port page.

---

---

### Remote Authentication

#### Note to CC-SG Users

When the KSX II is controlled by CommandCenter Secure Gateway, CC-SG authenticates users and groups, except for local users (requiring local port access). When CC-SG is controlling the KSX II, local port users will be authenticated against the local user database or the Remote Authentication server (LDAP/LDAPS or RADIUS) configured on the KSX II; they will not be authenticated against the CC-SG user database.

For additional information about CC-SG authentication, refer to the CommandCenter Secure Gateway User Guide, Administrator Guide, or Deployment Guide at:  
<http://www.raritan.com/support/productdocumentation>.

#### Supported Protocols

In order to simplify management of usernames and passwords, the KSX II provides the capability to forward authentication requests to an external authentication server. Two external authentication protocols are supported: LDAP/LDAPS and RADIUS.

#### Note on Microsoft Active Directory

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



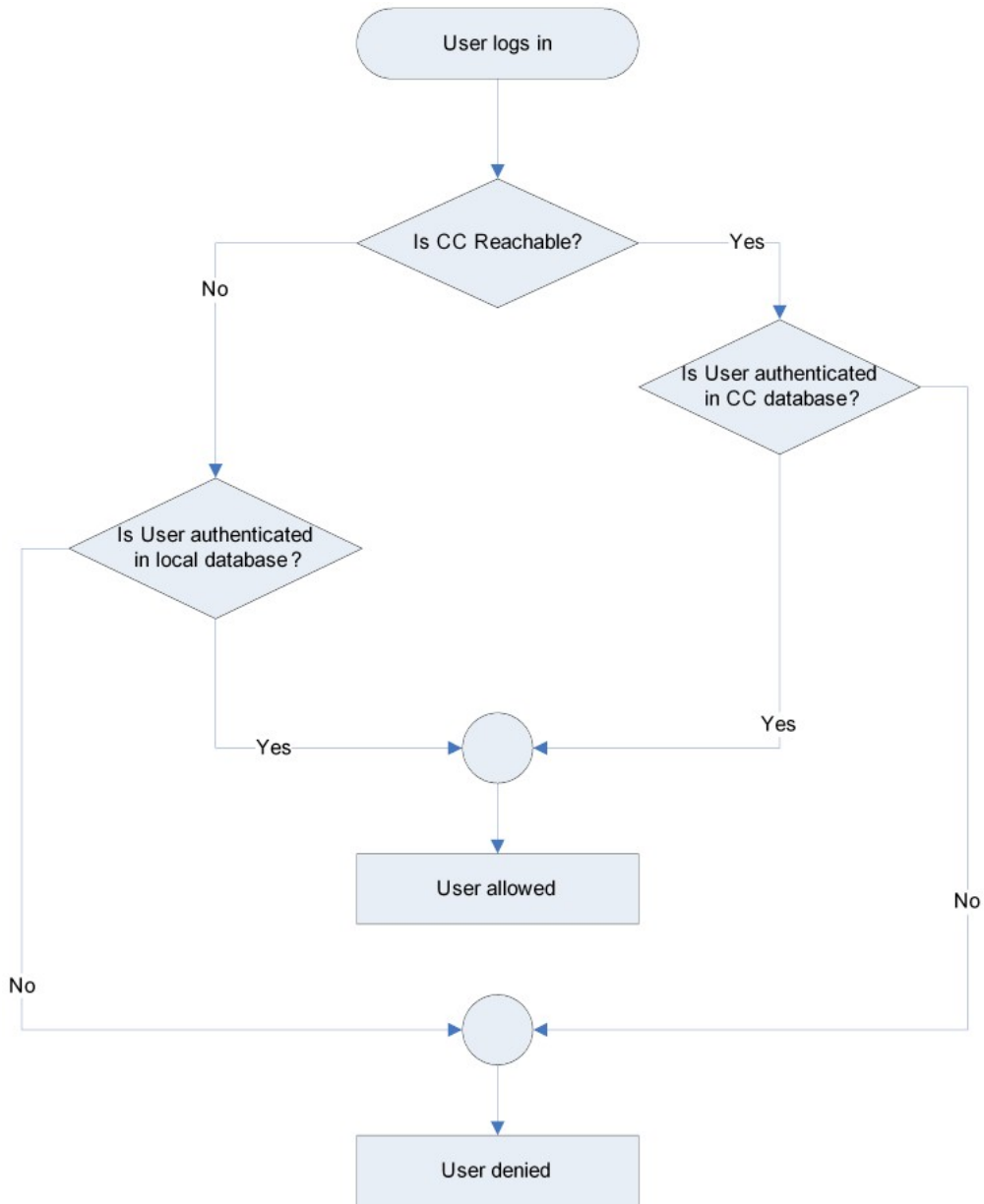
### Authentication vs. Authorization

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.

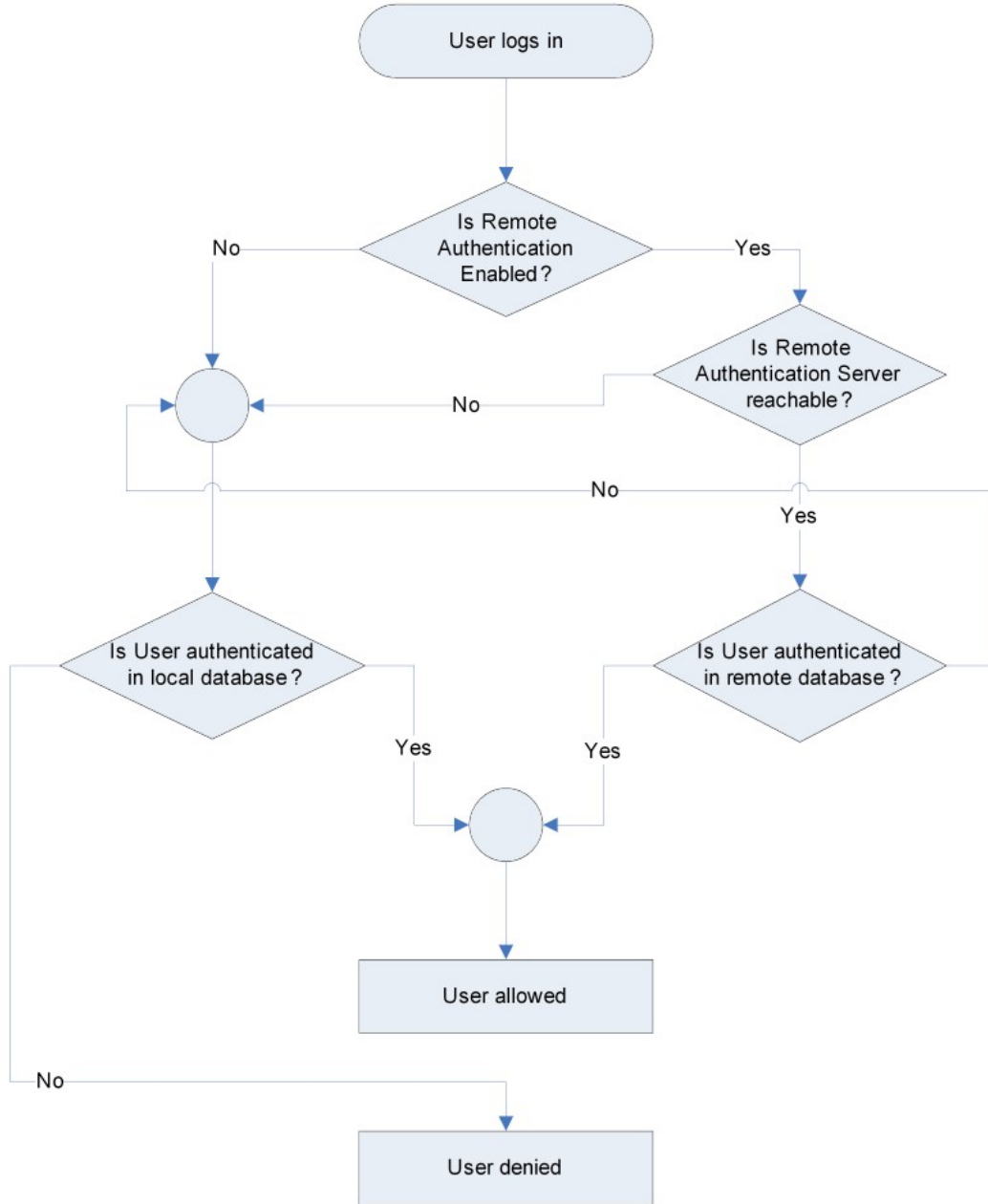
When KSX II is configured for remote authentication, the external authentication server is used primarily for the purposes of authentication, not authorization.

When the device is configured to authenticate and authorize local users from CC, the order in which the user credentials are validated follows the following process:

**Step 5: KSX II Initial Configuration**



Remote authentication follows the process specified in the flowchart below:



## Step 5: KSX II Initial Configuration

---

### Users, Groups, Relationships and Access Permissions

#### Users

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 KSX II is configured for LDAP/LDAPS or RADIUS, that authentication is processed first, followed by local authentication.

User names and passwords are required to gain access to the KSX II unit. This information is used to authenticate users attempting to access your KSX II unit. Refer to User Management for more information about adding and editing users.

#### Groups

Every KSX II unit is delivered with three default user groups; these groups cannot be deleted:

Admin	Users that are a member 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.

In addition to the system-supplied default groups, you can create groups and specify the appropriate permissions to suit your needs. Refer to User Management for more information about creating and editing user groups.

### 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 - which server ports are accessible, whether rebooting the unit is allowed, and other features.

### Users, Groups, and Access Permissions

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 KSX II is configured for LDAP/LDAPS or RADIUS, that authentication is processed first, followed by local authentication.

# Chapter 4 Connecting to the KSX II

## In This Chapter

User Interfaces.....	54
KSX II Local Console: KSX II Devices.....	55
Multi-Platform Client (MPC) .....	55
Language Support.....	56
Java Runtime Environment (JRE) .....	57
Launching the KSX II.....	57
Managing Favorites .....	62

---

## User Interfaces

There are several user interfaces in the KSX II providing you with easy access any time, anywhere. These include the KSX II Local Console and the Multi-Platform Client (MPC). The following table identifies these interfaces and their use for 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			✓	
Multi-Platform Client (MPC)			✓	✓
Raritan Serial Console (RSC)			✓	
Command Line Interface (CLI)	✓	✓	✓	✓

---

## KSX II Local Console: KSX II Devices

When you are located at the server rack, 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.

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 KSX II Local Console and the KSX II Remote Console user interfaces are almost identical; the following options are available in the KSX II Local Console, but not the KSX II Remote Console:

- **Local Port Settings** (see "Local Port Settings (KSX II Local Console Only)" on page 203)
- Factory Reset

---

## Multi-Platform Client (MPC)

The Raritan Multi-Platform Client (MPC) is a graphical interface that allows you to remotely access the target devices connected to Dominion units. MPC can be installed for standalone use or accessed through a web browser.

After installing the KSX II, either download a standalone version of Raritan MPC and establish an initial network connection, or launch the application directly.

---

*Note: MPC supports both KSX I and KSX II devices. Use MPC if you would like to access servers connected to both KSX I and KSX II devices with one user interface.*

---

➤ **To launch MPC directly:**

1. To launch MPC from a client running any browser, type `http://IP-ADDRESS/mpc` into the address line, where IP-ADDRESS is the IP address of your Raritan device. MPC will launch in a new window that does not contain a menu bar, tool bar, scroll bar, or address bar. Work in this window and toggle to other open windows using the ALT+TAB command.

## Language Support

2. When MPC launches, a device tree of all automatically detected Raritan devices found on your subnet is displayed on the left side of the screen. If you do not find your KSX II unit listed by name, create an icon manually by selecting Connection > New Profile. The Add Connection window opens.
3. Type a device Description, specify a Connection Type, add the Dominion unit's IP Address, and click OK. These specifications can be edited later.
4. In the Navigator panel on the left of the screen, double-click on the icon that corresponds to your KSX II unit.

Refer to the Raritan Multi-Platform Client (MPC) User Guide.

---

## Language Support

The KSX II provides keyboard support for the following languages: US English, UK English, Traditional Chinese, Simplified Chinese, Japanese, Korean, French, German, Belgian, Norwegian, Danish, and Swedish.

---

*Note: You can use the keyboard for Chinese, Japanese, and Korean for display only; local language input is not supported at this time for KSX II Local Console functions.*

---

For more information about non-US keyboards, see *Appendix C: Informational Notes* (see "Informational Notes" on page 285).

Language	Regions	Keyboard Layout
US English	United States of America and most of English-speaking countries: e.g. Canada, Australia, and New Zealand.	US Keyboard layout.
US English International	United States of America and most of English-speaking countries: e.g. 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



<b>Language</b>	<b>Regions</b>	<b>Keyboard Layout</b>
Japanese	Japan	JIS Keyboard
French	France	French (AZERTY) layout keyboard.
German	Germany and Austria	German keyboard (QWERTZ layout).
Belgium	Belgium	Belgian
Norway	Norway	Norwegian
Denmark	Denmark	Danish
Sweden	Sweden	Swedish

---

## **Java Runtime Environment (JRE)**

---

**Important: It is recommended that you disable Java caching and clear the Java cache. Please refer to your Java documentation or the Raritan Multi-Platform Client (MPC) User Guide for more information.**

---

The KSX II Remote Console and MPC require the JRE to function. 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.

Raritan recommends using Java Runtime Environment (JRE) version 1.5 for optimum performance, but the KSX II Remote Console and MPC will function with JRE version 1.4.2\_05 or greater (with the exception of JRE 1.5.0\_02), including JRE 1.6.

---

*Note: In order for multi-language keyboards to work in the KSX II Remote Console (Virtual KVM Client) please install the multi-language version of Java Runtime Environment (JRE).*

---

---

## **Launching the KSX II**

---

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

---

## Launching the KSX II

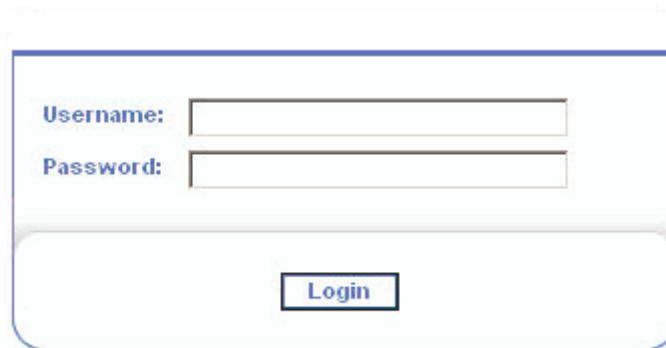
Depending on your browser and security settings, you may see various security and certificate warnings. It is necessary to accept these warnings to launch the KSX II Remote Console.

You can reduce the number of warning messages subsequent logins by checking the following on these security and certificate warning messages:

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

### ➤ **To launch the KSX II Remote Console:**

1. Log on to any workstation with network connectivity to your KSX II unit and Java Runtime Environment v1.4.2\_05 or higher installed (JRE is available at <http://java.sun.com/>).
2. Launch a supported web browser such as Internet Explorer (IE) or Firefox.
3. Type the following URL: `http://IP-ADDRESS`, where IP-ADDRESS is the IP Address that you assigned to your KSX II unit. You can also use `https`, the DNS name of the KSX II assigned by the administrator (provided that a DNS server has been configured), or just simply type the IP Address in the browser (KSX II always redirects the IP Address from HTTP to HTTPS.) The Login page opens:



4. Type your user name and password. If this is the first time logging in, log in with the factory default username and password (admin and raritan (all lower case)); you will be prompted to change the default password. Refer to Changing the Default Password for more information.
5. Click Login.

---

### **KSX II Console Layout**

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

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

---

### **KSX II Console Menus**

The below are examples of the menu options available in both the KSX II Remote and KSX II Local Console interfaces. These menus run along the top of the console page. Variations between the KSX II Local Console and the KSX II Remote Console are identified.

## Launching the KSX II

Port Access	Virtual Media	User Management	Device Settings	Security	Maintenance	Diagnostics
-------------	---------------	-----------------	-----------------	----------	-------------	-------------

Port Access	Virtual Media	User Management	Device Settings	Security	Maintenance	Diagnostics
-------------	---------------	-----------------	-----------------	----------	-------------	-------------

Note: Virtual Media is only available in the Remote Console.

Port Access	Virtual Media	User Management	Device Settings	Security	Maintenance	Diagnostics
		User List				
		Add New User				
		User Group List				
		Add New User Group				
		Change Password				
		Authentication Settings				

Port Access	Virtual Media	User Management	Device Settings	Security	Maintenance	Diagnostics
			Network			
			Device Services			
			Modem Settings			
			Date / Time			
			Event Management - Settings			
			Event Management - Destinations			
			Port Configuration			
			Port Keyword List			

Port Access	Virtual Media	User Management	Device Settings	Security	Maintenance	Diagnostics
				Security Settings		
				IP Access Control		

Port Access	Virtual Media	User Management	Device Settings	Security	Maintenance	Diagnostics
					Audit Log	
					Device Information	
					Backup / Restore	
					CIM Firmware Upgrade	
					Firmware Upgrade	
					Upgrade History	
					Reboot	

Note: The Backup/Restore and the Firmware Upgrade menu options are available in the Remote Console only. The Factory Reset option is available in the Local Console only.

Port Access	Virtual Media	User Management	Device Settings	Security	Maintenance	Diagnostics
						Network Interface
						Network Statistics
						Ping Host
						Trace Route to Host
						Device Diagnostics

Note: The KSX Diagnostics option is available in the Remote Console only.

The Favorites menu and the Help - User Guide link are located in the left panel of the page.

---

*Note: Both of these items are available in the Remote Console only.*

---

The Manage Favorite menu provides the following items:

- Favorites List
- Discover Devices - Local Subnet
- Discover Devices - KSX Subnet
- Add New Device to Favorites



See *Managing Favorites* (on page 62) for more information on managing favorites.

Following are variations between the KSX II Local Console and the KSX II Remote Console menu options:

Option	Local Console Only	Remote Console Only
Virtual Media		✓
File Server Setup		✓
Backup/Restore		✓
Firmware Upgrade		✓
Diagnostics		✓
Manage Favorites		✓
Favorites List		✓
Discover Devices - Local Subnet		✓

## Managing Favorites

Option	Local Console Only	Remote Console Only
Discover Devices - KSX II Subnet		✓
Add New Device to Favorites		✓
Help - User Guide		✓
Local Port Settings	✓	
Factory Reset	✓	

---

### Logging Out

➤ **To quit the KSX II Remote Console:**

- 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.*

---

---

## 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 name or IP Address
- Discover KSX II devices on its subnet (before and after login)
- Retrieve discovered KSX II devices from the connected KSX II device (after login)

---

*Note: This feature is available only on the KSX II Remote Console (not the KSX II Local Console).*

---

➤ **To access a favorite KSX II device:**

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

➤ **To toggle the Favorite Devices list display between name and IP Address:**

To display Favorites by IP Address:

- Click the Display by IP button.

Favorite Devices currently displayed by name; click Display by IP to toggle.

To display Favorites by name:

- Click the Display by Name button.

Favorite Devices currently displayed by IP Address; click Display by Name to toggle.



➤ **To open the Manage Favorites menu:**

- Click the Manage button. The Manage Favorites page opens and contains the following:

Use:	To:
Favorites List	Manage your list of favorite devices.
Discover Devices - Local Subnet	Discover the devices on the local subnet.
Discover Devices - KSX II Subnet	Discover the devices on the KSX II device subnet.
Add New Device to Favorites	Add, edit, and delete devices from your list of Favorites.

## Managing Favorites

The screenshot displays the Raritan Dominion KSX II web interface. The top navigation bar includes links for Port Access, Virtual Media, User Management, Device Settings, and Settings. The main content area is titled "Manage Favorites" and features a "Manage Favorites" header, a "Favorites List" section with links for "Discover Devices - Local Subnet", "Discover Devices - ksx2 Subnet", and "Add New Device To Favorites", and a "Favorite Devices" section listing "NewJersey\_RemoteOffice\_KSX" and "Sydney\_RemoteOffice\_KSX" with "Manage" and "Display By IP" buttons.

**Raritan.**

Port Access | Virtual Media | User Management | Device Settings | Settings

**Dominion® KSX II**

**Time & Session:**  
December 07, 2007 22:32:39

User: admin  
State: 3 min idle  
Your IP: 192.168.32.27  
Last Login: Dec 07, 2007 12:47

**Device Information:**  
Device Name: ksx2  
IP Address: 192.168.60.110  
Firmware: 1.0.0.5.6330

**Port States:**  
10 Ports up  
6 Ports down  
16 Ports idle

**Connected Users:**  
admin (192.168.32.27)  
3 min idle

[Help - User Guide](#)

**Favorite Devices:**  
NewJersey\_RemoteOffice\_KSX  
Sydney\_RemoteOffice\_KSX

[Manage](#)

[Display By IP](#)

Home > Manage Favorites

**Manage Favorites**

**Favorites List**

[Discover Devices - Local Subnet](#)

[Discover Devices - ksx2 Subnet](#)

[Add New Device To Favorites](#)

Copyright © 2007 Raritan Computer Inc.



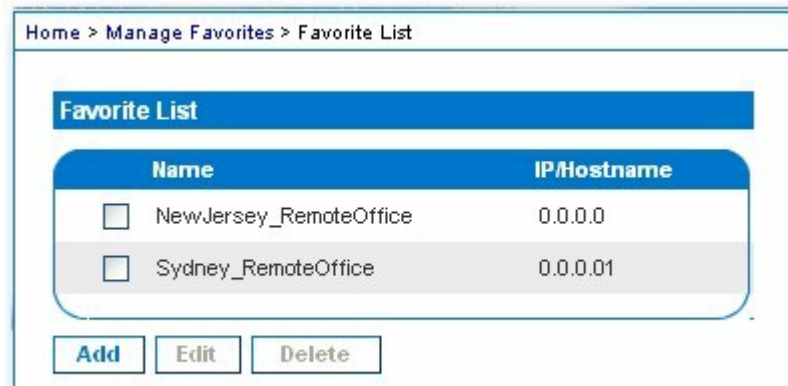
---

## Favorites List

From the Favorites List page, you can add, edit, and delete devices from your list of Favorites.

➤ **To open the Favorites List page:**

- Choose Manage > Favorites List. The Favorites List page opens:



➤ **To add a Favorite:**

- Click the Add button. The Add New Favorite page opens.

➤ **To delete a Favorite:**

---

**Important: Exercise caution in the removal of favorites; you are not prompted to confirm their deletion.**

---

6. Select the checkbox next to the appropriate KSX II device.
7. Click the Delete button. The favorite is removed from your list of favorites.

➤ **To edit a Favorite:**

8. From the Favorites List page, select the checkbox next to the appropriate KSX II device.
9. Click the Edit button. The Edit page opens:


## Managing Favorites

Home > Manage Favorites > Favorite List > Add New Favorite

### Add New Favorite

All fields are required

**Description**

  
**IP Address**  
**Port**  
**Product Type** 

10. Update the fields as necessary:
  - Description. Type something meaningful.
  - IP Address. Type the IP Address of the K5X II unit.
  - Port. Change the discovery Port (if necessary).
  - Product Type
11. Click OK.

### Discover Devices - Local Subnet

This option discovers the devices on your local subnet (that is, the subnet where the KSX II Remote Console is running). Access these devices directly from this page or add them to your list of favorites.

Discover Devices - Local Subnet

Use Default Port 5000

**Discover on Port:**

	Name	IP/Hostname
<input type="checkbox"/>	DominionKSX	192.168.50.78
<input type="checkbox"/>	DominionKX	192.168.50.240
<input type="checkbox"/>	KX_KIM-0050	192.168.50.12
<input type="checkbox"/>	shoaib-sx	192.168.50.239
<input type="checkbox"/>	shoaibkx2	192.168.50.234

➤ **To discover devices on the local subnet:**

1. Choose Favorites > Discover Devices - Local Subnet. The Discover Devices - Local Subnet page opens.
2. Select the appropriate discovery port (refer to Network Miscellaneous Settings for information about the discovery port):
  - To use the default discovery port, select the Use Default Port 5000 option.
  - To use a different discovery port:
    - a. Deselect the Use Default Port 5000 option.
    - b. Type the port number into the Discover on Port field.
    - c. Click Save.
3. Click Refresh. The list of devices on the local subnet is refreshed.

## Managing Favorites

➤ **To add devices to your Favorites List:**

1. Select the checkbox next to the device name/IP Address.
2. Click Add.

---

*Tip: Use the Select All and Deselect All buttons to quickly select all (or deselect all) devices in the remote console subnet.*

---

➤ **To access a discovered device:**

- Click the device name or IP address for that device. A new browser opens to that device.

### Discover Devices - KSX II Subnet

This option discovers the devices on the device subnet (that is, the subnet of the KSX II device IP address itself); access these devices directly from this page, or add them to your list of favorites.

This feature allows multiple KSX II units to interoperate and scale automatically. The KSX II Remote Console automatically discovers the KSX II units in the subnet of the KSX II.

The screenshot shows a web interface titled "Discover Devices - ksx2 Subnet". It features a table with two columns: "Name" and "IP/Hostname". Each row in the table has a checkbox on the left. Below the table are two buttons: "Select All" and "Deselect All". At the bottom right of the interface are two more buttons: "Add" and "Refresh".

	Name	IP/Hostname
<input type="checkbox"/>	6022	192.168.60.22
<input type="checkbox"/>	dksvg2-144	192.168.60.216
<input type="checkbox"/>	DominionKX	192.168.60.29
<input type="checkbox"/>	ewakX14G1	192.168.60.16
<input type="checkbox"/>	ewaskX2	192.168.60.20
<input type="checkbox"/>	KSX2	192.168.60.32
<input type="checkbox"/>	ksx2	192.168.60.110
<input type="checkbox"/>	KSX2-60-31	192.168.60.31
<input type="checkbox"/>	myEWAKSX2	192.168.60.18
<input type="checkbox"/>	myKX101EWA	192.168.60.17
<input type="checkbox"/>	PowerKX2	192.168.60.40
<input type="checkbox"/>	roykx25	192.168.60.25
<input type="checkbox"/>	roysksx2_30	192.168.60.30

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

1. Choose Favorites > Discover Devices - KSX II Subnet. The Discover Devices - KSX II Subnet page opens.
2. Click Refresh. The list of devices on the local subnet is refreshed.

## Managing Favorites

### ➤ **To add devices to your Favorites List:**

1. Select the checkbox next to the device name/IP Address.
2. Click Add.

---

*Tip: Use the Select All and Deselect All buttons to quickly select all (or deselect all) devices in the KSX II device subnet.*

---

### ➤ **To access a discovered device:**

- Click the device name or IP Address for that device. A new browser opens to that device.

---

## Add New Favorite

### ➤ **To add a device to your favorites list:**

1. Choose Manage Favorites > Add New Device to Favorites. The Add New Favorite page opens:
2. Type a meaningful description.
3. Type the IP Address for the device.
4. Change the discovery Port (if necessary).
5. Click OK.
6. This device is added to your list of favorites.
7. Select the product type.

8. Click OK. This device is added to your list of favorites.

Home > Manage Favorites > Favorite List > Add New Favorite

**Add New Favorite**

All fields are required

**Description**

  
**IP Address**  
**Port**  
**Product Type**

# Chapter 5 Accessing Target Servers

You are able to connect to KVM and serial devices using the following:

- Multi-Platform Client (MPC)
- Raritan Serial Client
- Via the Port Access Page

## In This Chapter

Port Access Page .....	73
Port Action Menu - KVM and Serial Ports .....	75
Connecting to a KVM Target Server .....	76
Connecting to a Serial Target Server.....	77
Switching Between KVM Target Servers.....	77
Disconnecting KVM and Serial Targets.....	77
Power Controlling a Target Server .....	78



## Port Access Page

After successfully logging into the KSX II Remote Console, the Port Access page opens. This page lists all of the KSX II ports, the connected KVM target servers and Serial target servers, and their status and availability. The Port Access page provides access to the KVM target servers and Serial target servers connected to the KSX II. KVM target servers and Serial target servers are servers that you want to control through the KSX II unit; they are connected to the KSX II ports at the back of the unit.

*Note: For each connection to a KVM target server, a new Virtual KVM Client window is opened. For each connection to a serial port, Raritan Serial Console (RSC) opens.*

### ➤ **To use the Port Access page:**

1. From the KSX II Remote Console, click the Port Access tab to open it. The Port Access page opens:

**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 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 unit. Please Note that ports connected to power strips will not be among those listed.

## Port Access Page

- Port Name. The name of the KSX II port; initially set to Dominion-KSX II-Port#, but you can change the name to something more descriptive. When you click on a Port Name link, the Port Action Menu is opened.
  - Port Type. Either Serial or KVM.
  - Status. The status is either up or down for KVM ports. The status is always up for serial ports.
  - Availability. The Availability can be Idle, Connected, Busy, or Unavailable. Availability depends on any active connection to the port.sd.
2. Click the Port Name of the target server you want to access. The Port Action Menu is displayed. Refer to Port Action Menu for more information about the menu options available.
  3. Select the desired menu option from the Port Action menu.
- **To change the display sort order:**
- Click the column heading you want to sort on. The list of target servers is sorted by that column.

## Port Action Menu - KVM and Serial Ports

When you click on a Port Name in the Port Access list, the Port Action menu is displayed. Please note that only options available for the selected port are listed in the Port Action menu:

The following table contains the possible menu options available in the Port Action menu. Note that the options vary slightly between KVM and serial ports:

Menu Item	Description	KVM	Serial
Connect	<p>Creates a new connection to the target server.</p> <p>For a KVM remote target, a new <i>Virtual KVM Client</i> (on page 81) window is opened and for a serial connection the Raritan Serial Client window will open.</p> <p>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.</p>	√	√
Switch From	<p>Switches from an existing connection to the selected port (KVM target server). This menu item is available only for KVM targets and is visible only when a virtual KVM client is opened.</p>	√	

*Note: This menu item is not available on the KSX II Local Console.*

## Connecting to a KVM Target Server

Menu Item	Description	KVM	Serial
Disconnect	Disconnects the port and closes the Virtual KVM Client window for the target server or, for serial connections, the Raritan Serial Client window for the target server. This menu item is available only when the port status is up and connected or up and busy. <hr/> <i>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 <b>hotkey</b> (see "Hotkeys" on page 201).</i>	√	√
Power On	Powers on the target server through the associated outlet.	√	√
Power Off	Powers off the target server through the associated outlets.	√	√
Power Cycle	<i>Power cycles the target server through the associated outlets.</i> <hr/> <i>Note: These power states are always visible when a port is associated with a target server.</i>	√	√

Select the desired menu option for that port to execute it.

---

## 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 is displayed.
3. Click Connect. A *Virtual KVM Client* (on page 81) window opens to the target server connected to that port.

---

## Connecting to a Serial Target Server

➤ **To connect to a serial 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 is displayed.
3. Select Connect. A Raritan Serial Console 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. 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 now. The Port Action menu is displayed.
3. Choose the Switch From option from the Port Action menu. The *Virtual KVM Client* (on page 81) window switches to the new target server you selected.

---

## Disconnecting KVM and Serial Targets

---

*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 **hotkey** (see "Hotkeys" on page 201).*

---

➤ **To disconnect a target server:**

1. Click the Port Name of the target you want to disconnect. The Port Action menu is displayed.
2. Choose the Disconnect option from the Port Action menu.

## Power Controlling a Target Server

---

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

*For serial connections, you can close the Raritan Serial Client by selecting Emulator > Exit.*

---

---

## Power Controlling a Target Server

---

*Note: These features are available only when you have made power associations. Refer to power control for more information.*

---

---

### Power Cycle a Target Server

- **To power cycle a KVM and/or serial target server:**
1. From the Remote Console or Local Console, click the Port Access tab to open it. The Port Access page opens.

- Click the Port Name of the appropriate target server. The Port Action menu is displayed.

**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
1	Win Target1	VM
2	Dominion_KSX2_Port2	Not
3	Dominion_KSX2_Port3	Not
4	KSX-G2 Admin	VM
5	Dominion_KSX2_Port5	Not
6	Dominion_KSX2_Port6	Not
7	Dominion_KSX2_Port7	Not
8	Dominion_KSX2_Port8	Not
9	co 2501	Serial
10	2	Serial
11	Serial Port 3	Serial
12	Serial Port 4	Serial
13	SP - 5	Serial
14	Serial Port 6	Serial
15	Serial Port 7	Serial
16	Serial Port 8	Serial

Connect  
 Power On  
 Power Off  
 Power Cycle

- Select Power Cycle. A message is displayed confirming the action taken.

---

### Power On a Target Server

➤ **To power ON a target server:**

- From the KSX II Remote Console, click the Port Access tab to open it. The Port Access page opens.
- Click the Port Name of the appropriate target server. The Port Action menu is displayed.
- Choose Power On.

## Power Controlling a Target Server

---

### Power Off a Target Server

➤ **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 is displayed.
3. Choose Power Off.



# Chapter 6 Virtual KVM Client

## In This Chapter

Overview .....	82
Options .....	83
Mouse Pointer Synchronization.....	85
Connection Menu.....	87
Keyboard Menu .....	90
Video Menu.....	95
Mouse Menu.....	99
Virtual Media .....	101
Tools Menu.....	102
View Menu.....	103
Help Menu.....	104

## Overview

---

## Overview

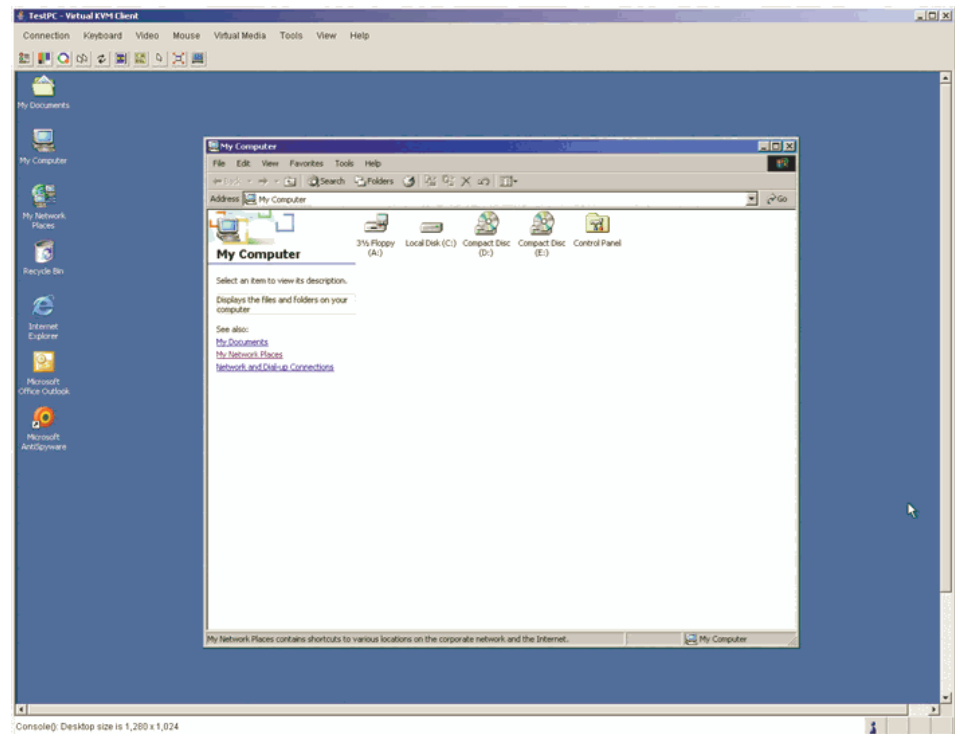
Whenever you access a target server using the KSX II Remote Console, a Virtual KVM Client window is opened. There is one Virtual KVM Client for each target server connected to; these windows can be accessed via the Windows Taskbar.

Virtual KVM Client windows can be minimized, maximized, and moved around your computer desktop.

---

*Note: Refreshing your HTML browser will close the Virtual KVM Client connection, so please exercise caution.*

---



The features available in the Virtual KVM Client are accessible through the menu and toolbar.

Feature	Description
Menu Bar	Drop-down menus of commands and settings.
Toolbar	Shortcut buttons to frequently used features and commands.

Feature	Description
Target Server Video Window	Target device display.
Status Bar	Real-time information on connection parameters, target server window size, concurrent connections, Caps Lock indicator, and Num Lock indicator.

---

## Options

---

### Menu Tree

The following list contains all of the menus and menu items available in the Virtual KVM Client.











- Connection
  - Properties
  - Connection Info
  - Exit
- Keyboard
  - Send Ctrl + Alt + Delete
  - Keyboard Macros
  - User-Created Macros (Optional)
- Video
  - Refresh Screen
  - Auto-Sense Video Settings
  - Calibrate Color
  - Video Settings
- Mouse
  - Synchronize Mouse
  - Single Mouse Cursor
  - Absolute
  - Intelligent
  - Standard

## Options

- Virtual Media
  - Connect Drive
  - Connect CD-ROM/ISO Image
- Tools
  - Options
- View
  - View Toolbar
  - Scaling
  - Target Screen Resolution
- Help
  - About Raritan Virtual KVM Client

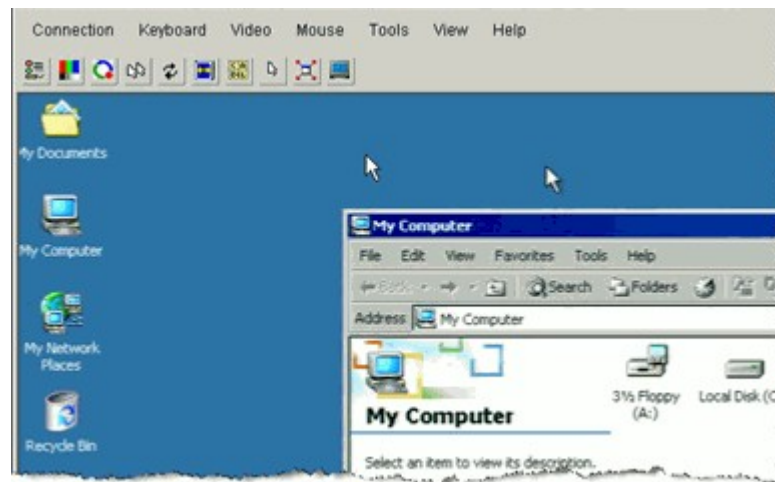
---

### Toolbar

Button	Description
	Properties
	Video settings
	Calibrate color
	Synchronize client and target server mouse cursors
	Refresh screen
	Auto-sense video
	Send Ctrl+Alt+Delete
	Toggles single/double mouse modes
	Full screen
	Resize video to fit screen

## Mouse Pointer Synchronization

When remotely viewing a target server that uses a mouse, you will see two mouse pointers: one belonging to your remote client workstation and the other belonging to the target server. When the mouse pointer lies within the Virtual 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 may want to disable the Virtual KVM Client mouse pointer and view only the target server's pointer. You can toggle between these two modes (single mouse and dual mouse). Refer to *Mouse Menu* (on page 99) for additional information about the available mouse modes.

### Mouse Synchronization Tips

Be sure to follow these steps when obtaining mouse synchronization:

1. Verify that the selected video resolution and refresh rate is among those supported by the KSX II. The Virtual KVM Client Connection Info dialog displays the actual values that the KSX II is seeing. Please refer to Supported Video Resolutions for more information about the video resolutions that are supported.
2. Verify that the cable length is within the specified limits for the selected video resolution. Please refer to *Target Server Connection Distance and Video Resolution* (on page 270) for more information.

## Mouse Pointer Synchronization

3. Verify that the mouse and video have been properly configured during the installation process. Please refer to *Chapter 3: Installation and Configuration* (see "Installation and Configuration" on page 19) for complete instructions.
4. Force an auto-sense by clicking the Virtual KVM Client auto-sense button.
5. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris KVM target servers):
  - a. Open a terminal window.
  - b. Enter the `xset mouse 1 1` command.
  - c. Close the terminal window.
6. Click the Virtual KVM Client mouse synchronization  button.

### **Additional Notes for Intelligent Mouse Mode**

- Be sure that there are no icons or applications in the upper left section of the screen since that is where the synchronization routine takes place.
- Do not use an animated mouse.
- Disable active desktop on KVM target servers.


---

## Connection Menu

---

### Properties Dialog

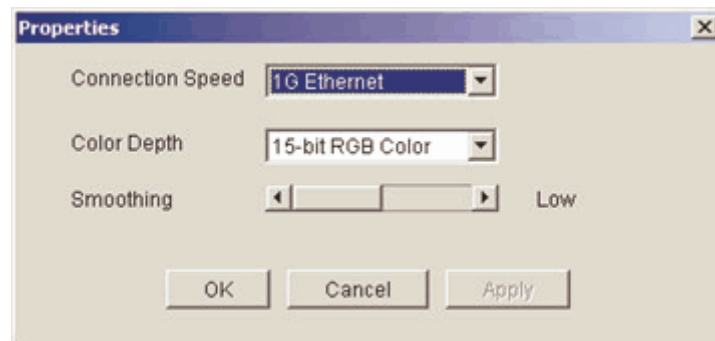
The KSX II dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. KSX II units optimize KVM output not only for LAN use, but also for WAN and dialup use. These units can also control color depth and limit video output, offering an optimal balance between video quality and system responsiveness for any bandwidth.

	Connection Properties	Manually adjust bandwidth-related options (connection speed, color depth, etc.).
---	-----------------------	--

The parameters in the Properties dialog can be optimized to suit your needs for different operating environments.

➤ **To set the connection properties:**

1. Choose Connection > Properties. The Properties dialog opens.



2. Select the Connection Speed from the drop-down list. KSX II can automatically detect available bandwidth and not limit bandwidth use; but you can also adjust this usage according to bandwidth limitations.

## Connection Menu

- 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)

Please 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.

1. Select the Color Depth from the drop-down list. KSX II 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, etc.), 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.

---



1. 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.
2. Click OK to set these properties.

➤ **To cancel without saving changes:**

- Click Cancel.

---

**Connection**

➤ **To obtain information about your Virtual KVM Client connection:**

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

The following information is displayed about the current connection:

- Device Name. The name of the KSX II device.
- IP Address. The IP Address of the KSX II 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 screen resolution horizontally.
- Vertical Resolution. The screen resolution vertically.
- Refresh Rate. How often the screen is refreshed.
- Protocol Version. RFB Protocol version.

➤ **To copy this information:**

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

## Keyboard Menu

---

### Exit

- **To close the Virtual KVM Client (the target you are currently accessing):**
  - Choose Connection > Exit.

---


## Keyboard Menu

---

### Send Ctrl+Alt+Delete

Due to its frequent use, a Ctrl+Alt+Delete macro has been pre-programmed into the Virtual KVM Client.

This key sequence is sent to the target server to which you are currently connected. In contrast, if you were to physically press the Ctrl+Alt+Delete keys while using the Virtual KVM Client, the command would first be intercepted by your own PC due to the structure of the operating system, instead of sending the key sequence to the target server as intended.

	Send Ctrl+Alt+Delete	Sends a Ctrl+Alt+Delete key sequence to the target server
---	----------------------	---

- **To send a Ctrl+Alt+Delete key sequence to the target server:**
  - Choose Keyboard > Send Ctrl+Alt+Delete, or
  - Click the Send Ctrl+Alt+Delete button from toolbar

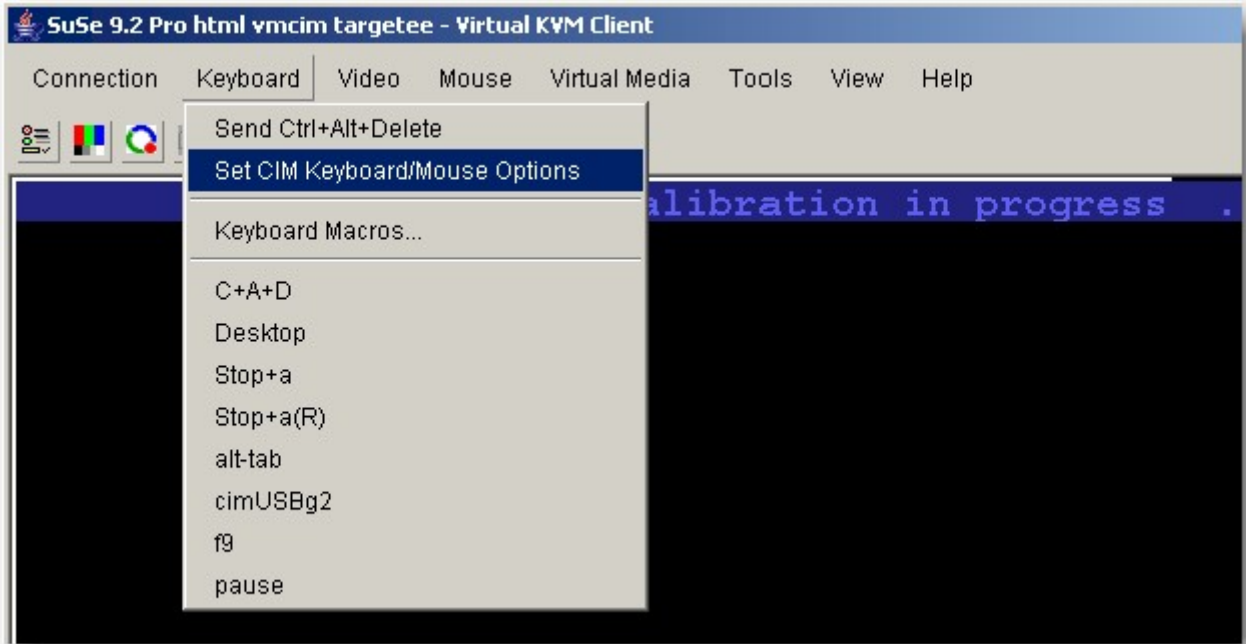
---

### Set CIM Keyboard/Mouse Options

To access the DCIM-USBG2 setup menu, perform the following steps.

1. Put the mouse focus on a window such as Note Pad (Windows) or an equivalent.
2. Press Left-Control and Numlock simultaneously. The CIM setup menu will appear in the active window.
3. Set the language and mouse settings.

4. Exit the menu to return to normal CIM functionality.



---

### 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 is running (your client PC).

Macros are stored on the client PC and are PC-specific; therefore, if you use another PC you will not 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 the Virtual KVM Client are available in MPC and vice versa.

---

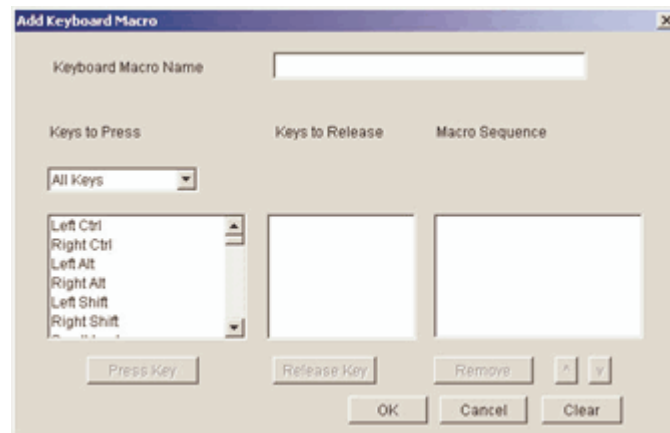
### Creating a Keyboard Macro

➤ **To create a keyboard macro (add a macro):**

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros window opens:



2. Click Add. The Add Keyboard Macro window opens:



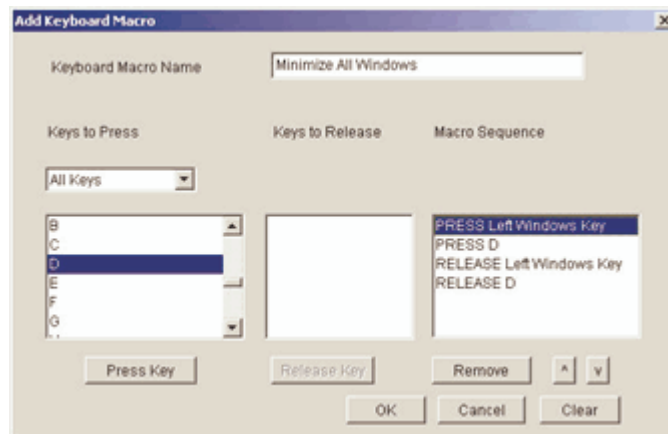
3. Type a name in the Keyboard Macro Name field. This is the name that will display on the Virtual KVM Client menu bar after the macro is created. In this example, type Minimize All Windows.
4. In the Keys to Press drop-down list:
  - a. Scroll through and select each key for which you would like to emulate a key press (in the order in which they are to be pressed).
  - b. Click the Press Key button after each selection. As each key is selected, it displays in the Keys to Release field.

In this example, select two keys: the Windows key and the letter D key.

5. In the Keys to Release field:
  - a. Choose each key for which you would like to emulate a key release (in the order in which they are to be released).
  - b. Click Release Key after each selection.

In this example, both keys pressed must also be released.

6. Review the Macro Sequence - which has been automatically generated using the Keys to Press and Keys to Release selections. Verify that the Macro Sequence is the exact key sequence you want. (To remove a step in the sequence, select it and click Remove.)

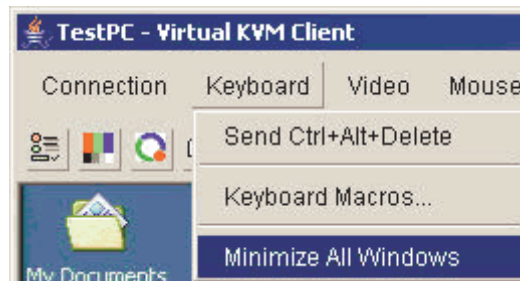


---

Tip: Use the ^ and v keys to reorder the key sequence.

---

7. Click OK in the Add Keyboard Macro window to save the macro.
8. Click Close from the Keyboard Macros window. The keyboard macro created is now listed as an option from Keyboard menu:



## Keyboard Menu

➤ **To cancel without saving changes:**

- Click Cancel.

➤ **To clear all fields and start over:**

- Click the Clear button.

---

### Running a Keyboard Macro

Once you have created a keyboard macro, execute it by clicking on its name in the Keyboard menu.

➤ **To execute a macro (using this example):**

- Choose Keyboard > Minimize All Windows.

An alternative method is to select the macro from the Keyboard Macros window.

➤ **To execute a macro:**

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros window opens.
2. Select the macro from among those listed.
3. Click Run Macro.

---

### Modifying a Keyboard Macro

➤ **To modify a macro:**

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros window opens.
2. Choose the macro from among those listed.
3. Click Modify. The Add/Edit Macro window opens.
4. Make your changes.
5. Click OK.

---

### Removing a Keyboard Macro

---

Please exercise caution in the removal of macros; you are not prompted to confirm their deletion.

---

➤ **To remove a macro:**

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros window opens.
2. Choose the macro from among those listed.
3. Click Remove. The macro is deleted.

---

## Video Menu

Video settings can be refreshed automatically in several ways:

- The Refresh Screen option forces a refresh of the video screen
- The Auto-sense Video Settings option automatically detects the target server's video settings
- The Calibrate Color option calibrates the video to enhance the colors being displayed

In addition, you can manually adjust the settings using the Video Settings option.

---

### Refresh Screen

The Refresh Screen option forces a refresh of the video screen. The entire video screen is redrawn.



➤ **To refresh the video settings:**

- Choose Video > Refresh Screen, or
- Click the Refresh Screen button from toolbar

---

### Auto-sense Video Settings

The Auto-sense Video Settings option forces a re-sensing of the video settings (resolution, refresh rate) and redraws the video screen.



➤ **To automatically detect the video settings:**

- Choose Video > Auto-sense Video Settings, or
- Click the Auto-Sense Video Settings button from toolbar

A message is displayed that auto adjustment is in progress.

## Video Menu

---

### Calibrate Color

Use the Calibrate Color command to optimize the color levels (hue, brightness, saturation) of the transmitted video images. The KSX II color settings are on a target server-basis.

	Calibrate Color	Adjusts color settings to optimize the video display.
---	-----------------	---

*Note: The Calibrate Color option applies to the current connection only.*

---

➤ **To calibrate the color:**

1. Open a remote KVM connection to any target server running a graphical user interface.
2. Choose Video > Calibrate Color (or click the Calibrate Color button). The target device screen updates its color calibration.

---

### Video Settings

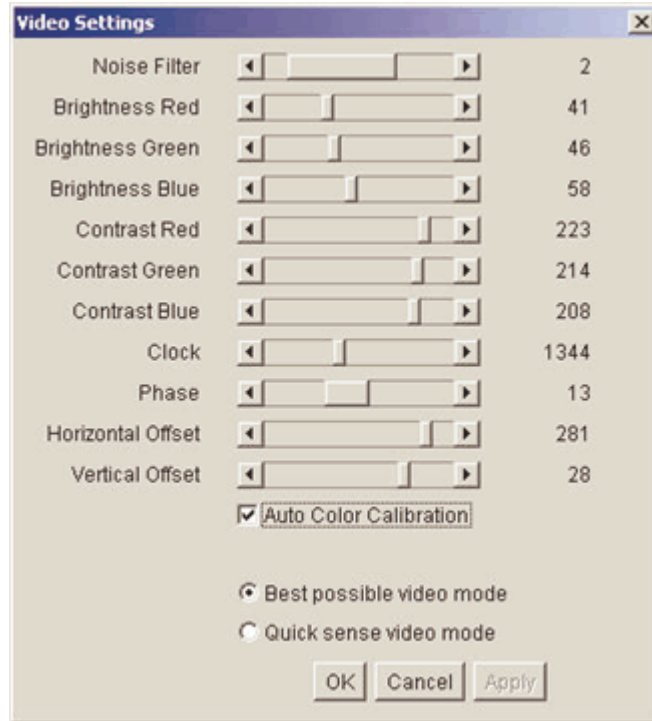
Use the Video Settings option to manually adjust the video settings.

	Video Settings	Opens Video Settings for manual adjustment of video parameters.
--	----------------	---



➤ **To change the video settings:**

1. Choose Video > Video Settings. The Video Settings window opens displaying the current settings:



2. Use the sliders to adjust the settings to achieve the desired results (as you adjust the settings the effects are immediately visible):
  - Noise Filter. KSX II can filter out the electrical interference of video output from graphics cards. This feature optimizes picture quality and reduces bandwidth. Higher settings transmit variant pixels only if a large color variation exists in comparison to the neighboring pixels. However, setting the threshold too high can result in the unintentional filtering of desired screen changes. Lower settings transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.
  - Brightness: Use this setting to adjust the brightness of the target server display.
    - Red. Controls the brightness of the red signal.
    - Green. Controls the brightness of the green signal.
    - Blue. Controls the brightness of the blue signal.
  - Color Contrast Settings: Controls the contrast adjustment.

## Video Menu

- Contrast Red. Controls the red signal.
- Contrast Green. Controls the green signal.
- 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: Please 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.

---

- 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 auto-detect 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.
  - Offset: Controls the on-screen positioning:
    - Horizontal Offset. Controls the horizontal positioning of the target server display on your monitor.
    - Vertical Offset. Controls the vertical positioning of the target server display on your monitor.
  - Auto Color Calibration. Check this option if you would like automatic color calibration.
  - Video Sensing: Select the video sensing mode:
    - Best possible video mode: KSX II 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 KSX II 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.
3. Click Apply. The Video Settings are changed.

---

*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.*

---

➤ **To cancel with saving your changes:**

- Click Cancel.

---

## Mouse Menu

When controlling a target server, the KSX II Remote Console displays two mouse cursors: one belonging to your client workstation and the other belonging to the target server. You can operate in either single mouse mode or dual mouse mode. When in dual mouse mode and properly configured, these two mouse cursors will align. If you experience difficulty with mouse synchronization, refer to *Configure Target Servers* (see "Step 1: Configure KVM Target Servers" on page 19).

When there are two mouse cursors, the KSX II offers several mouse modes:

- Absolute (Mouse Synchronization)
- Intelligent (Mouse Mode)
- Standard (Mouse Mode)

---

### Synchronize Mouse

In dual mouse mode, the Synchronize Mouse option forces realignment of the target server mouse pointer with Virtual KVM Client mouse pointer.



➤ **To synchronize the mouse:**

- Choose Mouse > Synchronize Mouse, or
- Click the Synchronize Mouse button from the toolbar

---

### Single Mouse Cursor

Single Mouse Cursor enters single mouse mode, in which only the target server mouse cursor is shown; the local PC mouse pointer no longer appears on-screen. While in single mouse mode, the Synchronize Mouse option is not available (there is no need to synchronize a single mouse cursor).

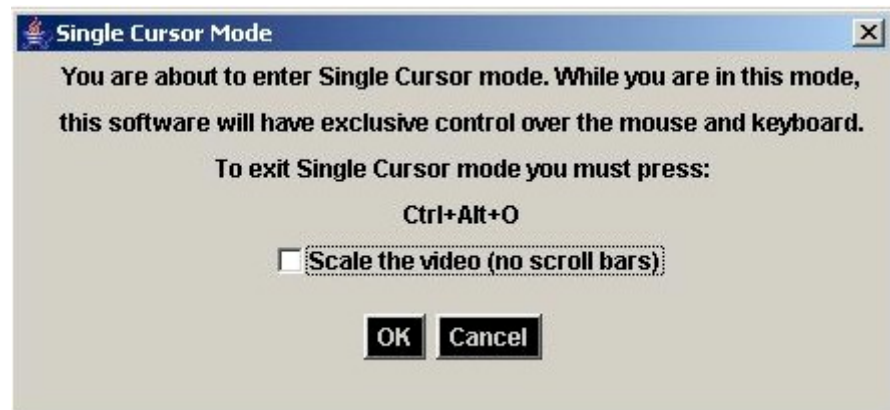


➤ **To enter single mouse mode:**

- Choose Mouse > Single Mouse Cursor, or
- Click the Single/Double Mouse Cursor button from the toolbar

➤ **To exit single mouse mode:**

4. When entering single mouse mode, the following message is displayed. Click OK.



5. Press Ctrl+Alt+O on your keyboard to exit single mouse mode.

---

### Standard

This is the standard mouse synchronization algorithm using relative mouse positions. Standard mouse mode requires that acceleration is disabled and other mouse parameters are set correctly in order for the client and server mouse to stay synchronized. Standard mouse mode is the default.

➤ **To enter standard mouse mode:**

- Choose Mouse > Standard.

---

## Intelligent

In Intelligent mouse mode, the KSX II can detect the target mouse settings and synchronize the mouse pointers accordingly, allowing mouse acceleration on the target. In this mode, the mouse cursor does a “dance” in the top left corner of the screen and calculates the acceleration. For this mode to work properly, certain conditions must be met.

For additional information on Intelligent Mouse mode, refer to the Raritan Multi-Platform Client User Guide (Appendix B: Conditions for Intelligent Mouse Synchronization) available on Raritan's Website <http://www.raritan.com/support/productdocumentation>, or on the Raritan User Manuals & Quick Setup Guides CD ROM included with your KSX II shipment.

➤ **To enter intelligent mouse mode:**

- Choose Mouse > Intelligent.

---

## Absolute

*Note: Absolute Mouse Synchronization is available for use with the Virtual Media-enabled USB CIM (D2CIM-VUSB) only.*

In this mode, absolute coordinates are used to keep the client and target pointers in sync, even when the target mouse is set to a different acceleration or speed. This mode is supported on servers with USB ports; the mouse moves to the exact location on the target server.

➤ **To enter absolute mouse mode:**

- Choose Mouse > Absolute.

---

## Virtual Media

Refer to the chapter on *Virtual Media* (on page 105) for complete information about setting up and using virtual media.

---

## Tools Menu

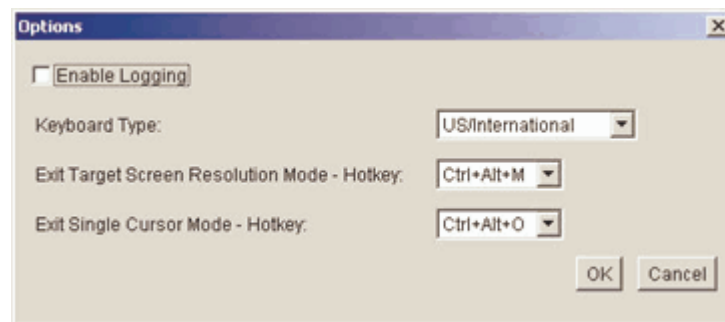
---

### Options

From the Tools menu, you can specify certain options for use with the Virtual KVM Client: synchronize mouse when in dual mouse mode, enable logging, keyboard type, and the exit target screen resolution mode hotkey.

➤ **To set the tools options:**

1. Choose Tools > Options. The Options window opens:



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)
  - Traditional and Simplified Chinese
  - German
  - Belgian
  - Norwegian
  - Danish
  - Swedish

4. Exit Target Screen Resolution Mode - Hotkey. When you enter target screen resolution mode, the display of the target server becomes full screen and acquires the same resolution as the target server. This is the hotkey used for exiting this mode; select from the drop-down list.
5. Exit Single Cursor Mode - Hotkey. When you enter single cursor mode, only the target server mouse cursor is visible. This is the hotkey used to exit single cursor mode and bring back the client mouse cursor; select from the drop-down list.
6. Click OK.

---

## View Menu

---

### 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.

---

### 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.

## Help Menu

---

### Target Screen Resolution

When you enter target screen resolution mode, the display of the target server becomes full screen and acquires the same resolution as the target server. The hotkey used for exiting this mode is specified in the Options dialog (default is Ctrl+Alt+M).

➤ **To enter target screen resolution:**

- Choose View > Target Screen Resolution.

➤ **To exit target screen resolution mode:**

- Press the hotkey configured in the Tools Options dialog. The default is Ctrl+Alt+M.

---

*Note to CC-SG Users: Target Screen Resolution is disabled; full screen mode is available only when the KSX II device is not under CC-SG management.*

---

---

## Help Menu

---

### About Raritan Virtual KVM Client

This menu option provides version information about the Virtual KVM Client should you require assistance from Raritan technical support.

➤ **To obtain version information:**

- Choose Help > About Raritan Virtual KVM Client.



# Chapter 7 Virtual Media

## In This Chapter

Overview .....	106
Prerequisites for Using Virtual Media.....	108
Using Virtual Media .....	109
Opening a KVM Session.....	110
Connecting to Virtual Media.....	112
Disconnecting Virtual Media .....	115
File Server Setup (File Server ISO Images Only).....	116

---

## Overview

Virtual media extends KVM capabilities by enabling KVM target servers to remotely access media from the client PC and network file servers. With this feature, media mounted on the client PC and network file servers is 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. Virtual media can include internal and USB-mounted CD and DVD drives, USB mass storage devices, PC hard drives, and ISO images (disk images).

---

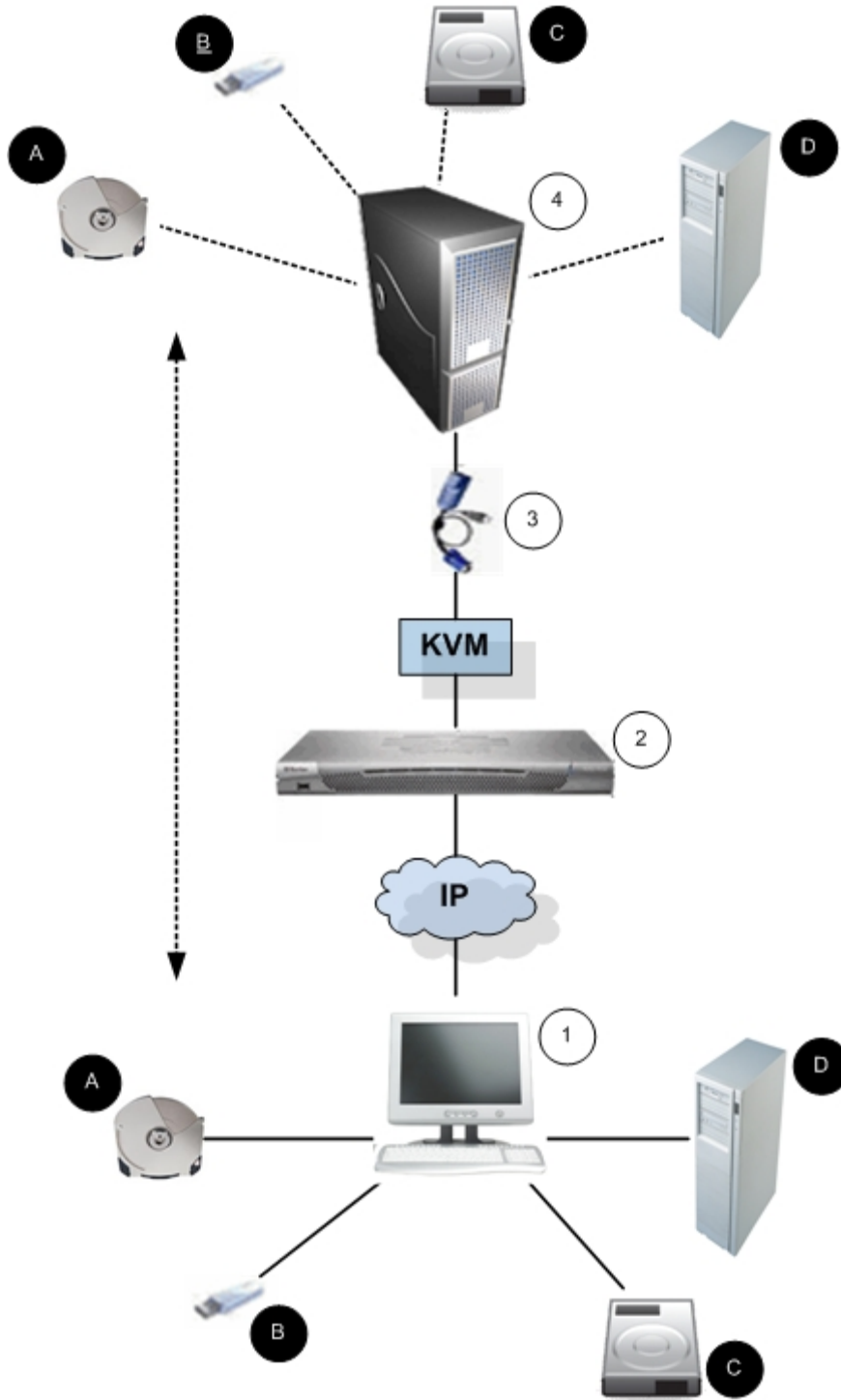
*Note: ISO9660 is the standard supported by Raritan. However, other ISO standards can be used.*

---

Virtual media provides the ability to perform additional tasks remotely, such as:

- transferring files
- running diagnostics
- installing or patching applications
- complete installation of the operating system

This expanded KVM control eliminates most trips to the data center, saving time and money, thereby making virtual media very powerful.



## Prerequisites for Using Virtual Media

Item	Description
1	Desktop PC
2	KSX II
3	CIM
4	Target Server
A	CD/DVD Drive
B	USB
C	Hard Drive Image Files
D	Remote File Server (ISO Images)

---

## Prerequisites for Using Virtual Media

The following conditions must be met in order to use virtual media:

### **KSX II**

- For users requiring access to virtual media, 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; please refer to Setting Port Permissions for more information.
- (Optional) If you want to use PC-Share, VM Share Mode must also be enabled in the Security Settings page.

### **Client PC**

- Certain virtual media options require administrative privileges on the client PC (e.g., drive redirection of complete drives).

---

Note: If you are using Microsoft Vista, turn User Account Control off: Control Panel > User Accounts > User Account Control > turn off.

---

---

If you would prefer not to change Vista account permissions, run Internet Explorer as an administrator. To do this, click on the Start Menu, locate IE, right click it and select Run as Administrator.

---

- USB 2.0 ports are both faster and preferred.

#### Target Server

- KVM target servers must support USB connected drives.
- KVM target servers running Windows 2000 must have all of the recent patches installed.

---

## Using Virtual Media

With the KSX II virtual media feature, you can mount up to two drives (of different types). 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.

#### ➤ **To use virtual media:**

1. 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.
2. Verify that the appropriate *prerequisites* (see "Prerequisites for Using Virtual Media" on page 108) are met.
3. (File server ISO images only) If you plan to access file server ISO images, identify those file servers and images through the KSX II Remote Console *File Server Setup page* (see "File Server Setup (File Server ISO Images Only)" on page 116).

---

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

---

4. Open a KVM session with the appropriate target server.
5. Connect to the virtual media.

#### **For:**

Local drives

#### **Select this VM option:**

*Connect Drive* (see "Local Drives" on page 112)

## Opening a KVM Session

For:	Select this VM option:
Local CD/DVD drives	<i>Connect CD-ROM/ISO Image</i> (see "CD-ROM/DVD-ROM/ISO Images" on page 114)
ISO Images	Connect CD-ROM/ISO Image
File Server ISO Images	Connect CD-ROM/ISO Image

6. Upon completion of your tasks, *disconnect the virtual media* (see "Disconnecting Virtual Media" on page 115).

---

## Opening a KVM Session

➤ **To open a KVM session:**

1. Open the Port Access page from the KSX II Remote Console.
2. Connect to the target server from the Port Access page:
  - a. Click the Port Name for the appropriate server.
  - b. Choose the Connect option from the Port Action Menu.

The target server opens in a *Virtual KVM Client* (on page 81) window.

**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
1	<a href="#">Connect target1</a>	VM
2	Dominion_KSX2_Port2	Not
3	Dominion_KSX2_Port3	Not
4	KSX-G2 Admin	VM
5	Dominion_KSX2_Port5	Not
6	Dominion_KSX2_Port6	Not
7	Dominion_KSX2_Port7	Not
8	Dominion_KSX2_Port8	Not
9	Cisco 2501	Serial
10	SP-2	Serial
11	Serial Port 3	Serial
12	Serial Port 4	Serial
13	SP - 5	Serial
14	Serial Port 6	Serial
15	Serial Port 7	Serial
16	Serial Port 8	Serial

---

## Connecting to Virtual Media

---

### Local Drives

This option mounts an entire drive; 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. This is the only option for which Read-Write is available.

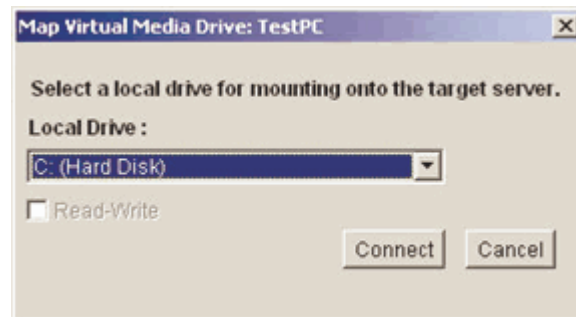
---

*Note: KVM target servers running certain version of the Windows operating system may not accept new mass storage connections after an NTFS-formatted partition (e.g., the local C drive) has been redirected to them. If this occurs, close the KVM II 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.*

---

➤ **To access a drive on the client computer:**

1. From the Virtual KVM Client, select Virtual Media > Connect Drive. The Map Virtual Media Drive dialog opens:



2. Choose the drive from the Local Drive drop-down list.
3. If you want read and write capabilities, select the Read-Write option checkbox. This option is disabled for non-removable drives. Please refer to the *conditions when read-write is not available* (on page 113) for more information. When checked, you will be able to read or write 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.

---



4. Click Connect. The media will be mounted on the target server virtually. You can access the media just like any other drive.

---

Note: If there is no USB connection to the target server, you will see a warning message that says, "The virtual media capability is set up but will not be available until the USB cable is connected or the target is powered on. Please check your USB connectivity or see if the target is powered on." Resolve this issue, then connect to the drive again.

---

---

### **Conditions when Read-Write is not Available**

Virtual media read-write is not available in the following situations:

- For all hard drives.
- 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

## Connecting to Virtual Media

---

### CD-ROM/DVD-ROM/ISO Images

This option mounts CD-ROM, DVD-ROM, and ISO images.

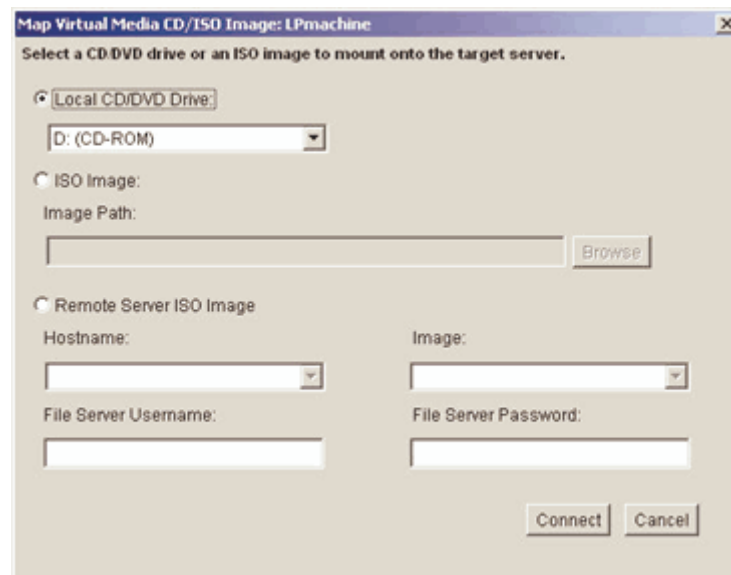
---

*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. The Map Virtual Media CD/ISO Image dialog opens:



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 the Browse button.
  - 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 lists. The file servers and image paths available are those that you configured using the File Server Setup page. Only items you configured using the KSX II File Server Setup page will be in the drop-down list.
    - c. File Server Username. Username required for access to the file server.
    - 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.

---

## Disconnecting Virtual Media

➤ **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 option, simply closing the KVM connection closes the Virtual Media as well.*

---

## File Server Setup (File Server ISO Images Only)

---

### File Server Setup (File Server ISO Images Only)

---

*Note: This feature is only required when using virtual media to access file server ISO images.*

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

---

Use the KSX II Remote Console File Server Setup page to designate the files server(s) and image paths that you want to access using KSX II Virtual Media. File server ISO image(s) specified here will become 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 "CD-ROM/DVD-ROM/ISO Images" on page 114)).

➤ **To designate file server ISO images for virtual media access:**

1. Choose Virtual Media from the KSX II Remote Console. The File Server Setup page opens:

Selected	Host Name/IPAddress	Image Path
<input checked="" type="checkbox"/>	192.168.1.193	/images/disk1.iso
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

Save Cancel

2. Enter information about the file server ISO images that you want to access:

- Host Name/IP Address. Host name or IP Address of the file server.
  - Image Path. Full path name of the location of the ISO image.
3. Select the Selected checkbox for all media that you want accessible as virtual media.
  4. Click Save. All media specified here will now be available for selection in the Map Virtual Media CD/ISO Image dialog.
- **To cancel without saving:**
- Click Cancel.

# Chapter 8 User Management

## In This Chapter

User Management Menu .....	118
User List.....	119
Adding a New User .....	120
User Group List.....	122
Add New User Group .....	123
Change Password .....	131
Authentication Settings .....	132

---

## User Management Menu

The User Management menu is organized as follows: User List, Add New User, User Group List, Add New User Group, Change Password, and Authentication Settings.

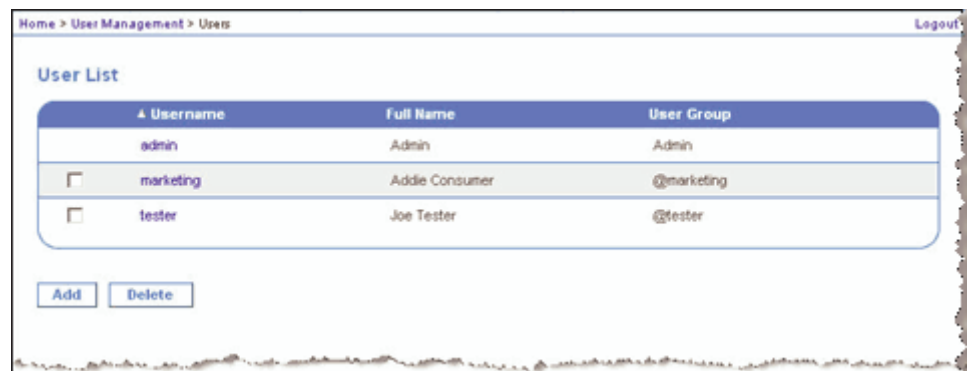
<b>Use:</b>	<b>To:</b>
User List	Display an alphabetical list of all users; add, modify, or delete users.
Add New User	Add new users; modify user information.
User Group List	Display an alphabetical list of all user groups; add, modify, or delete user groups.
Add New User Group	Add new user groups; modify user group information.
Change Password	Change password for a specific user.
Authentication Settings	Configure the type of authentication used for access to the KSX II.

## User List

The User List page displays a list of all users including their Username, 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 also add, modify, or delete users.

➤ **To view the list of users:**

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



➤ **To add a new user:**

- Click the Add button. The User page opens. For complete information about the User page, refer to Add New User.

➤ **To modify an existing user:**

1. Locate the user from among those listed.
2. Click on the Username. The User page opens. For complete information editing the user, refer to *Modify Existing User* (on page 121).

➤ **To delete a user:**

1. Select the user from among those listed by selecting the checkbox to the left of the Username.
2. Click Delete. You are prompted to confirm the deletion.
3. Click OK.

---

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

---

*Note: A username can be deactivated (Active checkbox is deselected when the number of failed login attempts has exceeded the maximum login attempts set in the Security Settings screen. Refer to **Security Settings** (on page 168) for more information.*

---

➤ **To add a new user:**

1. Open the User page using one of these methods:
  - Choose User Management > Add New User, or
  - Click the Add button on the User List page.

Home > User Management > User

**User**

Username <sup>\*</sup>

Full Name

Password <sup>\*</sup>

Confirm Password <sup>\*</sup>

Dialback Number

User Group <sup>\*</sup>

--- select ---

Active

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; 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 in will fail when it is attempted:
  - " double quote
  - ' single quote
  - ; semicolon
  - \$ dollar sign
  - & and sign
  - | 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 *Set Permissions for Individual Group* (on page 131).
7. To activate the new user, select the Active checkbox. The default is activated (enabled).
8. Click OK.

---

### **Modify Existing User**

➤ **To modify an existing user:**

1. In the User page, change the appropriate fields. (Refer to Add New User for information about how to get access the User page.)
2. Click OK.

---

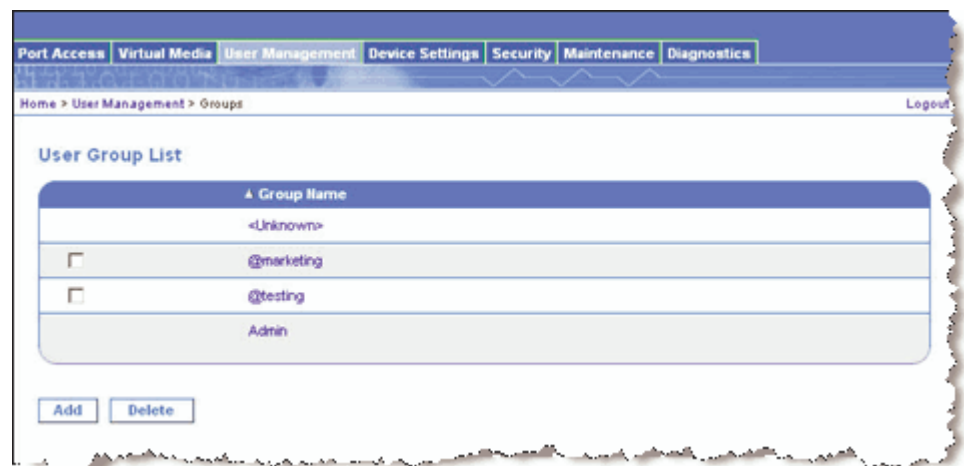
## User Group List

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, because 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:



➤ **To add a new user group:**

- Click the Add button. The Group page opens. For complete information about the Group page, refer to *Add New User Group* (on page 123).

➤ **To modify an existing user group:**

1. Locate the user group from among those listed.
2. Click on the Group Name. The Group page opens. For complete information editing the group, refer to *Modify Existing User Group*.

➤ **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.

---

## **Add New User Group**

➤ **To add a new user group:**

1. Open the Group page using one of these methods:
  - Choose User Management > Add New User Group, or

## Add New User Group

- Click the Add button from the User Group List page

Home > User Management > Group Logout

### Group

Group Name \*

#### Permissions

- Device Settings
- Diagnostics
- Maintenance
- Modem Access
- PC-Share
- Security
- User Management

#### Port Permissions

Port	Access	VM Access	Power Control
Win Target	Deny	Deny	Deny
Dominion_KSX2_Port2	Deny	Deny	Deny
Dominion_KSX2_Port3	Deny	Deny	Deny
KSX-G2 Admin	Deny	Deny	Deny
Dominion_KSX2_Port5	Deny	Deny	Deny
Dominion_KSX2_Port6	Deny	Deny	Deny
Dominion_KSX2_Port7	Deny	Deny	Deny
Dominion_KSX2_Port8	Deny	Deny	Deny
Cisco 2501	Deny		Deny
SP-2	Deny		Deny
Serial Port 3	Deny		Deny
Serial Port 4	Deny		Deny
SP - 5	Deny		Deny
Serial Port 6	Deny		Deny
Serial Port 7	Deny		Deny
Serial Port 8	Deny		Deny

Set All to Deny     Set All VM Access to Deny     Set All Power to Deny  
 Set All to View     Set All VM Access to Read-Only     Set All Power to Access  
 Set All to Control     Set All VM Access to Read-Write

#### IP ACL

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

Copyright © 2007 Raritan Computer Inc.

The Group page is organized into the following categories: Group, Permissions, Port Permissions, and IP ACL.

- Type a descriptive name for the new user group into the Group Name field.

3. 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. Refer to Setting Permissions for more information.
4. Set the Port Permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). Refer to Setting Port Permissions for more information.
5. *Set the IP ACL* (see "Group-based IP ACL (Access Control List)" on page 126) (optional). 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* (on page 176) list feature which applies to all access attempts to the device (and takes priority).
6. Click OK.

---

*Note: Several administrative functions are available within MPC and from the KSX II Local Console; these functions are available only to members of the default ADMIN group.*

---



---

### **Setting Permissions**

---

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

---

<b>Permission</b>	<b>Description</b>
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 device.
PC-Share	Simultaneous access to the same target by multiple users
Security	SSL certificate, security settings (VM Share, PC-Share), IP ACL

## Add New User Group

Permission	Description
User Management	User and group management, remote authentication (LDAP/LDAPS/RADIUS), login settings

### Setting Port Permissions

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

Access		VM Access		Power Control	
Option	Descrip.	Option	Descrip.	Option	Descrip.
None*	Denied access completely	Deny*	Virtual media permission is denied altogether for the port	Deny*	Deny power control to the target server
View	View the video (but not interact with) the connected target server	Read-Only	Virtual media access is limited to read access only	Access	Full permission to power control on a target server
Control	Control the connected target server	Read-Write	Complete access (read, write) to virtual media		

\* Default setting

*Tip: Use the checkboxes to quickly set all the permissions the same for every port.*

### Group-based IP ACL (Access Control List)

**Important:** Please 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 which applies to all access attempts to the device, is processed first, and takes priority. Refer to *IP Access Control* (on page 176) for more information.

**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

Append   Insert   Replace   Delete

➤ **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 specifying accept are allowed access to the KSX II device.
  - Drop. IP Addresses specifying drop are denied access to the KSX II device.
4. Click Append. The rule is added to the bottom of the rules list.
5. Repeat steps 1 through 4 for each rule you want to enter.

➤ **To insert a rule:**

1. Type a Rule #. A Rule # is required when using the Insert command.
2. Type the Starting IP and Ending IP fields.
3. Choose the Action 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.

## Add New User Group

### ➤ **To replace a rule:**

1. Specify the Rule # 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 #.

### ➤ **To delete a rule:**

1. Specify the Rule # 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.**

---

IP ACL			
Rule #	Starting IP	Ending IP	Action
1	192.168.50.1	192.168.55.255	ACCEPT
2	0.0.0.0	255.255.255.255	DROP
<input type="text"/>	<input type="text"/>	<input type="text"/>	ACCEPT ▾
<input type="button" value="Append"/> <input type="button" value="Insert"/> <input type="button" value="Replace"/> <input type="button" value="Delete"/>			

---

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

---



---

## **Modify Existing User Group**

---

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

---

➤ **To modify an existing user group:**

1. From the Group page, change the appropriate fields and set the appropriate permissions.

## Add New User Group

Home > User Management > Group Logout

**Group**

Group Name ^

**Permissions**

Device Settings  
 Diagnostics  
 Maintenance  
 Modem Access  
 PC-Share  
 Security  
 User Management

**Port Permissions**

Port	Access	VM Access	Power Control
Win Target	Deny	Deny	Deny
Dominion_KSX2_Port2	Deny	Deny	Deny
Dominion_KSX2_Port3	Deny	Deny	Deny
KSX-G2 Admin	Deny	Deny	Deny
Dominion_KSX2_Port5	Deny	Deny	Deny
Dominion_KSX2_Port6	Deny	Deny	Deny
Dominion_KSX2_Port7	Deny	Deny	Deny
Dominion_KSX2_Port8	Deny	Deny	Deny
Cisco 2501	Deny		Deny
SP-2	Deny		Deny
Serial Port 3	Deny		Deny
Serial Port 4	Deny		Deny
SP - 5	Deny		Deny
Serial Port 6	Deny		Deny
Serial Port 7	Deny		Deny
Serial Port 8	Deny		Deny

Set All to Deny     
  Set All VM Access to Deny     
  Set All Power to Deny  
 Set All to View     
  Set All VM Access to Read-Only  
 Set All to Control     
  Set All VM Access to Read-Write     
  Set All Power to Access

**IP ACL**

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

Copyright © 2007 Raritan Computer Inc.

- 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. Refer to Setting Permissions for more information.
- Set the Port Permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). Refer to Setting Port Permissions for more information.

4. Set the IP ACL (optional). This feature limits access to the KSX II device by specifying IP addresses. Refer to *Group-based IP Access Control List* (see "Group-based IP ACL (Access Control List)" on page 126) for more information.
5. Click OK.

---

### Set Permissions for Individual Group

➤ **To set permissions for an individual user group:**


1. Locate the user 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.

---

### Change Password

➤ **To change your password:**

1. Choose User Management > Change Password. The Change Password page opens:



2. Type your current password in the Old Password field.

## Authentication Settings

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, refer to **Security Settings - Strong Passwords** (see "Strong Passwords" on page 171).*

---

---

## Authentication Settings

From the Authentication Settings page you can configure the type of authentication used for access to your KSX II. Refer to Authentication vs. Authorization for more information about how authentication and authorization operate and differ.

---

*Note: Even if you select remote authentication (LDAP/LDAPS or RADIUS), local authentication is still used.*

---

➤ **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** (on page 135) 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 138) for information about completing the fields in the RADIUS section of the Authentication Settings page.
6. Click OK to save.

➤ ***To cancel without saving changes:***

- Click Cancel.

➤ ***To return to factory defaults:***

- Click the Reset to Defaults button.

## Authentication Settings

### Authentication Settings

Local Authentication  
 LDAP

Primary LDAP Server

Secondary LDAP Server

Secret Phrase

Confirm Secret Phrase

Dialback Query String

Enable Secure LDAP

Port

Secure LDAP Port

Certificate File

DN of Administrative User

User Search DN

Type of External LDAP Server

Active Directory Domain

RADIUS

Primary RADIUS Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Secondary RADIUS Server

Shared Secret

Authentication Host

---

### Implementing LDAP Remote Authentication

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

---

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

---

➤ **To use the LDAP authentication protocol, enter the following information:**

1. Type the IP Address or DNS name of your LDAP/LDAPS remote authentication server in the Primary LDAP Server field. When the Enable Secure LDAP option is selected, the DNS name must be used.
2. (Optional) Type the IP Address or DNS name of your backup LDAP/LDAPS server in the Secondary LDAP Server field. When the Enable Secure LDAP option is selected, the DNS name must be used. Please note that the remaining fields share the same settings with the Primary LDAP Server field.
3. Type the server secret (password) required to authenticate against your remote authentication server in the Secret Phrase field and again in the Confirm Secret Phrase field. Enter the password in use on the LDAP/LDAPS server.
4. Dialback Query String. Type the dialback query string. If you are using Microsoft Active Directory, you must enter the following string:

msRADIUSCallbackNumber

---

Note: This string is case sensitive.

---

5. Select the Enable Secure LDAP checkbox if you would like to use SSL; the Secure LDAP Port field is enabled. Secure Sockets Layer (SSL) is a cryptographic protocol which allows K5X II to communicate securely with the LDAP/LDAPS server.
6. The default Port is 389. Either use the standard LDAP TCP port or specify another port.
7. The default Secure LDAP Port is 636. Either use the default port or specify another port. This field is enabled when the Enable Secure LDAP checkbox is selected.

## Authentication Settings

8. Certificate File. Consult your authentication server administrator to get the CA certificate file in Base64 encoded X-509 format for the LDAP/LDAPS server. Use the Browse button to navigate to the certificate file. This field is enabled when the Enable Secure LDAP option is selected.
9. DN of administrative User. Distinguished Name of administrative user; 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".
10. User Search DN. This describes the name you want to bind against the LDAP/LDAPS, and where in the database to begin searching for the specified Base DN. 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.
11. Type of 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.
12. Active Directory Domain. Type the name of the Active Directory Domain.



---

## 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).

---

*Note: If you are an existing Raritan, Inc. customer, and have already configured the Active Directory server by changing the AD schema, KSX II still supports this configuration, and you do not need to perform the following operations. Please refer to Appendix B: Updating the LDAP/LDAPS Schema for information about updating the AD LDAP/LDAPS schema.*

---

➤ **To enable your AD server on the KSX II:**

1. Using KSX II, create special groups and assign proper permissions and privileges to these groups. For example, create groups such as: KVM\_Admin, 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. Refer to *Implementing LDAP/LDAPS Remote Authentication* (see "Implementing LDAP Remote Authentication" on page 135).

---

### Important Notes:

---

- Group Name is case sensitive.
- The KSX II provides the following default groups which can not be changed or deleted: Admin and <Unknown>. Please 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 a 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

### 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:**

The screenshot shows a configuration window titled "RADIUS". It contains two identical sections for "Primary Radius Server" and "Secondary Radius Server". Each section has the following fields: "Primary Radius Server" (text input), "Shared Secret" (text input), "Authentication Port" (text input with value 1812), "Accounting Port" (text input with value 1813), "Timeout (in seconds)" (text input with value 1), and "Retries" (text input with value 3). At the bottom, there is a "Global Authentication Type" dropdown menu with "PAP" selected.

1. Type the IP Address of your primary and (optional) secondary remote authentication servers in the Primary Radius Server and Secondary Radius Server fields, respectively.
2. Type the server secret used for authentication (in the Shared Secret fields). 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.
3. Authentication Port. The default authentication port is 1812; change as required.

4. Accounting Port. The default accounting port is 1813; change as required.
5. Timeout (in seconds). The default timeout is 1 second; change 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.
6. Retries. The default number of retries is 3; change as required. This is the number of times the KSX II will send an authentication request to the RADIUS server.
7. Global Authentication Type. Choose from among the options in the drop-down list:
  - PAP. With PAP, passwords are sent as plain text. PAP is not interactive; the username 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.

---

### Returning User Group Information via RADIUS

When a RADIUS authentication attempt succeeds, the KSX II device 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};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 unit sends the following RADIUS attributes to your RADIUS server:

Attribute	Data
<b>Login</b>	
Access-Request (1)	

## Authentication Settings

Attribute	Data
<b>Login</b>	
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-IP-Address (4)	The IP Address for the KSX II unit.
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 unit.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
<b>Logout</b>	
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 unit.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

# Chapter 9 Device Management

## In This Chapter

Device Settings Menu .....	141
Network Settings .....	142
Device Services.....	146
Modem Settings .....	148
Date/Time Settings.....	149
Event Management.....	150
Port Configuration Page.....	158

---

## Device Settings Menu

The Device Settings menu is organized as follows:

Use:	To:
Network	Customize the network configuration for the KSX II.
Device Services	Configure direct port access and miscellaneous network settings.
Modem Settings	Configure modem settings.
Date/Time	Set date, time, time zone, and Network Time Protocol (NTP).
Event Management - Settings	Configure SNMP and Syslog.
Event Management - Destinations	Select which system events to track and where to send this information.
Port Configuration	Configure KVM ports, power CIMs, and outlets.
Local Port Settings	Configure local port; KSX II Local Console
Port Keywords	Create port keywords and associated them

## Network Settings

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

**Important: Before changing the network configuration, ensure that there are no other active user connections to the device; all connections will be dropped when the KSX II unit is reconfigured.**

Basically, there are two ways to setup your IP Configuration:

- None. This option 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. The IP Address is automatically assigned by a DHCP server.

➤ **To change the network configuration:**

1. Chose Device Settings > Network. The Network Settings page opens.

The screenshot shows the 'Network Settings' page with two main sections: 'Network Basic Settings' and 'LAN Interface Settings'. The 'Network Basic Settings' section includes fields for Device Name (PM\_KSX2), IP auto configuration (None), Preferred host name (DHCP only), IP address (192.168.59.248), Subnet mask (255.255.255.0), Gateway IP address (192.168.59.126), Primary DNS server IP address, and Secondary DNS server IP address. The 'LAN Interface Settings' section includes a note about reliable communication, current LAN interface parameters (autonegotiation on, 10 Mbps, half duplex, no link), LAN Interface Speed & Duplex (Autodetect), Enable Automatic Failover, Ping Interval (seconds) (30), Timeout (seconds) (60), and Bandwidth Limit (No Limit). There is a 'Set System ACL' button and 'OK', 'Reset To Defaults', and 'Cancel' buttons at the bottom.

2. Update the Network Basic Settings. Refer to Network Basic Settings for more information about each of the fields.
3. Update the LAN Interface Settings. Refer to LAN Interface Settings for more information about each of the fields.

4. Click OK to set these configurations. If your changes require rebooting the device, a reboot message appears.

➤ **To cancel without saving changes:**

- Click Cancel.

➤ **To reset to factory defaults:**

- Click Reset to Defaults.

---

### Network Basic Settings

- Device Name. Type a unique name for the device (up to 16 characters; spaces are not allowed). Name your device so you can easily identify it. The default name for a KSX II unit is: "DominionKSX". Remote users will also see this name. However, if an MPC user has created a Connection Profile for this device, that user will see the Description field from the Profile instead.
- IP auto configuration. Select from among the options available in the drop-down list:
  - None. Use this option if you do not want an auto IP configuration and prefer to set the IP Address yourself (static IP). This is the default and recommended option.

---

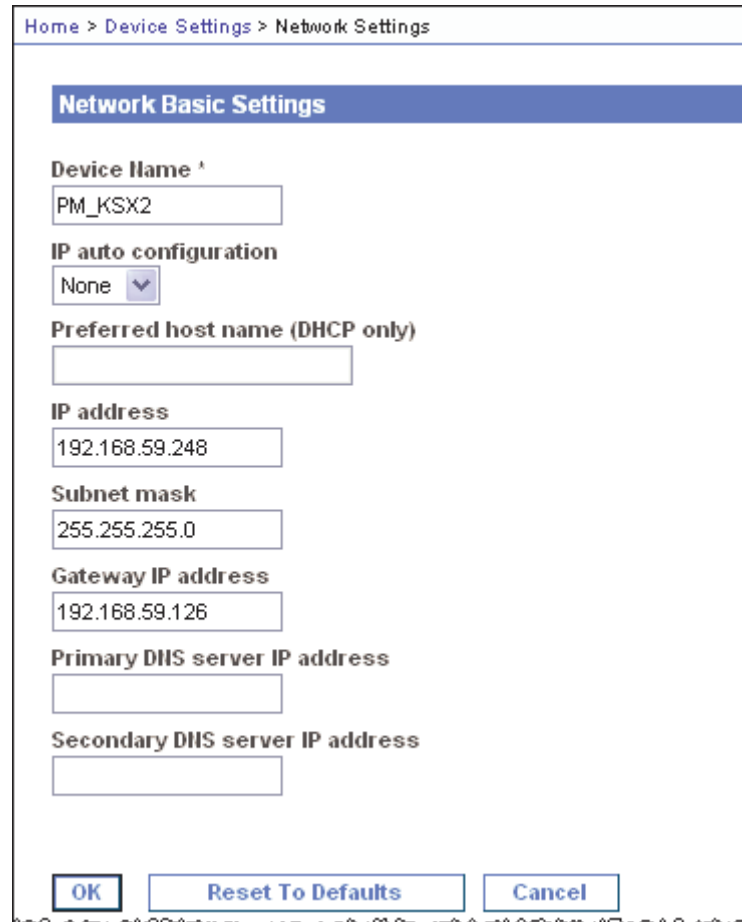
If this option is selected for the IP auto configuration, the following Network Basic Settings fields are enabled, allowing you to manually set the IP configuration.

---

- IP Address. The default IP Address is 192.168.0.192.
- Subnet Mask. The default subnet mask is 255.255.255.0.
- Gateway IP Address. The IP Address for the gateway (if one is used).
- Primary DNS Server IP Address. The primary Domain Name Server used to translate names into IP Addresses.
- Secondary DNS Server IP Address. The secondary Domain Name Server used to translate names into IP Addresses (if one is used).
- DHCP. Dynamic Host Configuration Protocol is used by networked computers (clients) to obtain unique IP addresses and other parameters from a DHCP server.

## Network Settings

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



The screenshot shows a web-based configuration interface for network settings. At the top, a breadcrumb trail reads "Home > Device Settings > Network Settings". Below this is a blue header bar labeled "Network Basic Settings". The form contains several fields: "Device Name" with the value "PM\_KSX2"; "IP auto configuration" set to "None" via a dropdown menu; "Preferred host name (DHCP only)" which is currently empty; "IP address" set to "192.168.59.248"; "Subnet mask" set to "255.255.255.0"; "Gateway IP address" set to "192.168.59.126"; "Primary DNS server IP address" which is empty; and "Secondary DNS server IP address" which is also empty. At the bottom of the form are three buttons: "OK", "Reset To Defaults", and "Cancel".



### LAN Interface Settings

LAN Interface Settings

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

**Current LAN interface parameters:**  
autonegotiation on, 10 Mbps, half duplex, no link

**LAN Interface Speed & Duplex**

Autodetect ▼

Enable Automatic Failover

**Ping Interval (seconds) ^**

**Timeout (seconds) ^**

**Bandwidth Limit**

No Limit ▼

Set System ACL

- The current parameter settings are identified in the Current LAN interface parameters field.
- LAN Interface Speed & Duplex. Select from among the speed and duplex combinations available.
 

Autodetect	Default option
10 Mbps/Half	
10 Mbps/Full	
100 Mbps/Half	
100 Mbps/Full	
1000 Mbps/Full	Gigabit

  - 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.

## Device Services

---

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

---

Please refer to *Network Speed Settings* (on page 271) for more information.

- Enable Automatic Failover. Check this checkbox to allow KSX II to automatically recover its network connection using a second network port if the active network port fails. When this option is enabled, the following two fields are used:
  - Ping Interval (seconds). Ping interval determines how often KSX II checks the status of the network connection (setting this too low may cause excess network traffic). The default Ping Interval is 30 seconds.
  - Timeout (seconds). Timeout determines how long a network port must be “dead” before the switch is made. Both network ports must be connected to the network and this option must be checked for Automatic Failover to function. The default Timeout is 60 seconds.

---

Note: The default Ping Interval and Timeout generate a condition that when the KSX II device tries to switch over, remote sessions will be dropped and must be re-established. Reducing these intervals to much lower values will allow remote sessions to stay connected, but will result in increased network traffic.

---

- Set System ACL. Click this button to set a global-level Access Control List for your KSX II by ensuring that your device does not respond to packets being sent from disallowed IP addresses. The *IP Access Control* (on page 176) page opens.

---

Note: These ACL values are global, affecting the KSX II unit as a whole. You can also create ACLs on a group-level basis. For example, you can create an “Outsourced Vendors” user group that is permitted to access KSX II only from a given IP address range (refer to *Group-based IP ACL* (see “Group-based IP ACL (Access Control List)” on page 126) for more information on how to create group-specific Access Control Lists).

---

## Device Services

1. Choose Device Settings > Device Services. The Device Service Settings page appears.
2. Enter or select the following:

- Discovery Port. 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 unit from beyond a firewall, your firewall settings must enable two-way communication through the default port 5000 or a non-default port configured here.
- Enable Telnet Access. Check this option to allow Administrators to access the KSX II via Telnet.
- Telnet Port. The standard Telnet port number is 23 but it can be changed to provide a higher level of security operations.
- Enable SSH Access. Check this option to allow Administrators to access the KSX II via the SSH v2 application.
- SSH Port. The standard SSH TCP port number is 22 but the port number can be changed to provide a higher level of security operations.
- Enable Serial Console Access. Select this option to allow Administrators to activate the local serial console port.
- Baud Rate. The speed of the local serial console port connection.

Home > Device Settings > Device Services

Services		Direct Port Access				
Discovery Port *	5000	Port Number	Port Name	IP Address	SSH TCP Port	Telnet TCP Port
<input type="checkbox"/> Enable TELNET Access		9	Cisco 2501		2209	
TELNET Port	23	10	SP-2			
<input checked="" type="checkbox"/> Enable SSH Access		11	Serial Port 3			
SSH Port	22	12	Serial Port 4			
<input type="checkbox"/> Enable Serial Console Access		13	SP - 5			
Baud Rate:	9600	14	Serial Port 6			
		15	Serial Port 7			
		16	Serial Port 8			

OK    Reset To Defaults    Cancel

---

### Modem Settings

➤ **To configure modem settings:**

1. Click Device Settings > Modem Settings to open the Modem Settings page.
2. Complete the following fields as needed:
  - Enable Modem
  - PPP Server IP Address - the internet address assigned to the KSX II when a connection is established via dial-up. Required.
  - 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.

---

- Enable Modem Dialback

---

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 a user that does not have a call back number defined in their profile.

---

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

**Modem Settings**

**Enable Modem**

PPP Server IP Address  
10.1.1.2

PPP Client IP Address  
10.1.1.3

**Enable Modem Dialback**

OK    Reset To Defaults    Cancel

## Date/Time Settings

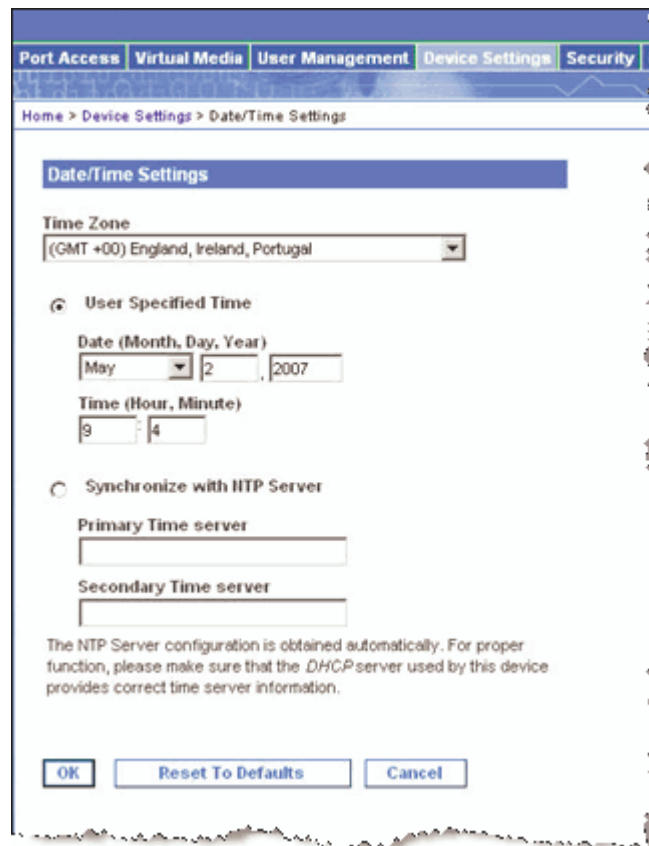
Use the Date/Time Settings page to specify the date and time for the KSX II. There are two ways to do this:

- Manually set the date and time, or
- Synchronize with a Network Time Protocol (NTP) Server.

*Note: The KSX II does not support Daylight Savings Time.*

### ➤ **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. Choose the method you would like to use to set the date and time:
  - User Specified Time. Choose this option to input the date and time manually.

## Event Management

- Synchronize with NTP Server. Choose this option to synchronize the date and time with the Network Time Protocol (NTP) Server.
4. For the User Specified Time option, enter the date and time as follows:
    - a. Choose the Month from the drop-down list.
    - b. Type the Day of the Month.
    - c. Type the Year in yyyy format.
    - d. Type the Time in hh:mm format (using a 24-hour clock).
  5. For the Synchronize with NTP Server option:
    - a. Enter the IP address of the Primary Time server.
    - b. (Optional) Enter the IP address of the Secondary Time server.
  6. Click OK.

---

## Event Management

The KSX II Event Management feature provides a set of screens for enabling and disabling the distribution of system events to SNMP Managers, 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.

## Event Management - Settings

### SNMP Configuration

Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions. KSX II offers SNMP Agent support through Event Management. Refer to SNMP Agent Configuration and SNMP Trap Configuration for more information about SNMP Agents and Traps.

➤ **To configure SNMP (enable SNMP logging):**

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page opens:

The screenshot shows a web interface for configuring SNMP. At the top, there are navigation tabs: Port Access, Virtual Media, User Management, Device Settings (selected), Security, and Maintenance. Below the tabs is a breadcrumb trail: Home > Device Settings > Event Management - Settings. The main content area is titled "SNMP Configuration" and contains the following fields:

- SNMP Logging Enabled
- Name:
- Contact:
- Location:
- Agent Community String:
- Type:

Below these fields is a table with three columns: Destination IP, Port #, and Community. The table contains five rows, each with the value "162" in the Port # column and empty cells in the other two columns.

Below the table is a link: [Click here to view the Dominion-IOX2 SNMP MIB](#)

The bottom section is titled "SysLog Configuration" and contains:

- Enable Syslog Forwarding
- IP Address:

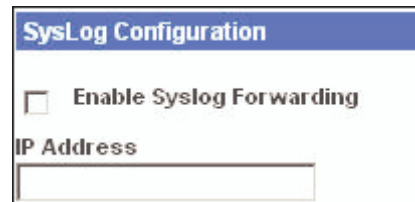
At the bottom of the page are three buttons: OK, Reset To Defaults, and Cancel.

2. Choose the Enable SNMP Logging option; this enables the remaining SNMP fields.

## Event Management

3. In the Name, Contact, and Location fields, type the SNMP Agent's (this Dominion unit's) name as it appears in the KSX II Console interface, a contact name related to this unit, and where the Dominion unit is physically located, respectively.
4. Type the Agent Community String (the Dominion unit's string). An SNMP community is the group that devices and management stations running SNMP belong to; it helps define where information is sent. The community name is used to identify the group; an SNMP device or agent may belong to more than one SNMP community.
5. Specify whether the community is Read-Only or Read-Write using the Type drop-down list.
6. Configure up to five SNMP managers by specifying their Destination IP, Port #, and Community.
7. Click the [Click here to view the Dominion- SNMP MIB link](#) to access the SNMP Management Information Base.
8. Click OK.

## Syslog Configuration



- **To configure the Syslog (enable Syslog forwarding):**
1. Choose the Enable Syslog Forwarding option to log the device's messages to a remote Syslog server.
  2. Type the IP Address of your Syslog server in the IP Address field.
  3. Click OK.



➤ **To cancel without saving changes:**

- Click Cancel.

➤ **To reset to factory defaults:**

- Click the Reset To Defaults button.

---

**Event Management - Destinations**

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

---

*Note: SNMP traps will only be generated if the SNMP Logging Enabled option is checked; Syslog events will only be generated if the Enable Syslog Forwarding option is checked. Both of these options are in the Event Management - Settings page.*

---

➤ **To select events and their destinations:**

1. Choose Device Settings > Event Management - Destinations. The Event Management - Destinations page opens:

## Event Management

Home > Device Settings > Event Management - Destinations

### Event Management - Destinations

Note: SNMP traps will only be generated if the "SNMP Logging Enabled" option is checked. Similarly, Syslog events will only be generated if the "Syslog Forwarding" option is checked. These options can be found on the "Event Management - Settings" page on the Device Settings menu.

Category	Event	SNMP	Syslog	Audit
Device Operation		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Startup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Powerstrip Outlet Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Parameter Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Ethernet Failover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Management		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	FactoryReset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Begin CC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	End CC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Started	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Completed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

System events are categorized by Device Operation, Device Management, Security, User Activity, and User Group Administration.

2. Check 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 line checkboxes, respectively.

---

3. Click OK.
  - **To cancel without saving changes:**
    - Click Cancel.
  - **To reset to factory defaults:**
    - Click the Reset To Defaults button.

**SNMP Trap Configuration**

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
cimConnected	A CIM is plugged into to the KSX II port.
cimDisconnected	A CIM is either unplugged from the KSX II port or powered-off.
cimUpdateCompleted	CIM firm ware update process completed.
cimUpdateStarted	CIM firm ware update process started.
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.
ethernetFailover	An Ethernet failover was detected and restored on a new Ethernet interface.
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.

## Event Management

Trap Name	Description
ipConflictResolved	An IP Address conflict was resolved.
networkFailure	An Ethernet interface of the product can no longer communicate over the network.
networkParameterChanged	A change has been made to the network parameters.
passwordSettingsChanged	Strong password settings have changed.
portConnect	A previously authenticated user has begun a KVM session.
portConnectionDenied	A connection to the target port was denied.
portDisconnect	A user engaging in a KVM session closes the session properly.
portStatusChange	The port has become unavailable.
powerNotification	The power outlet status notification: 1=Active, 0=Inactive.
powerOutletNotification	Power strip device outlet status notification.
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.
securityViolation	Security violation.
startCCManagement	The device has been put under CommandCenter Management.
stopCCManagement	The device has been removed from CommandCenter Management.
sxPortAlert	Logs keywords and sends out an event.
userAdded	A user has been added to the system.
userAuthenticationFailure	A user attempted to log in without a correct username and/or password.

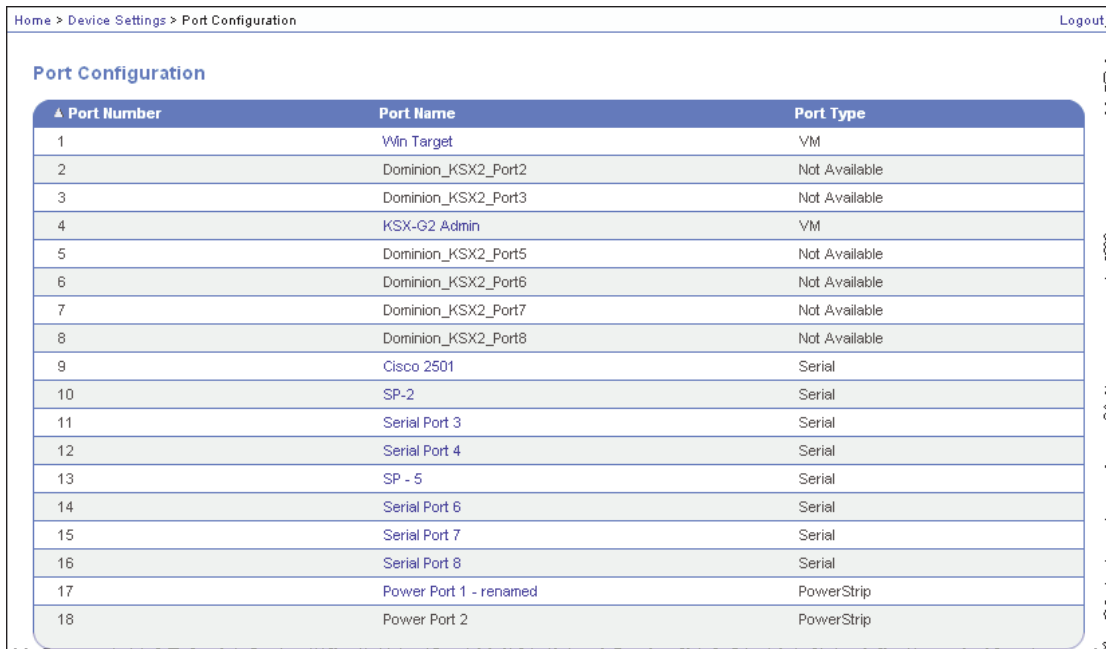
Trap Name	Description
userConnectionLost	A user with an active session has experienced an abnormal session termination.
userDeleted	A user account has been deleted.
userLogin	A user has successfully logged into the KSX II and has been authenticated.
userLogout	A user has successfully logged out of the 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.
vmImageConnected	User attempted to mount either a device or image on the target using Virtual Media. For every attempt on device/image mapping (mounting) this event is generated.
vmImageDisconnected	User attempted to unmount a device or image on the target using Virtual Media.

## Port Configuration Page

The Port Configuration page displays a list of the KSX II ports. Ports connected to KVM and serial target servers or power strips are displayed in blue and can be edited. For ports with no CIM connected or with a blank CIM name, a default port name of KSX II\_Port# is assigned, where Port# is the number of the KSX II physical port.

➤ **To access the Port Configuration page:**

1. Choose Device Settings > Port Configuration. The Port Configuration Page opens:



The screenshot shows a web interface for 'Port Configuration'. At the top, there is a breadcrumb trail 'Home > Device Settings > Port Configuration' and a 'Logout' link. Below the breadcrumb is the title 'Port Configuration'. The main content is a table with three columns: 'Port Number', 'Port Name', and 'Port Type'. The table contains 18 rows of data. The 'Port Name' column uses color coding: black text for non-editable names and blue text for editable names. The 'Port Type' column lists various connection types like VM, Not Available, Serial, and PowerStrip.

Port Number	Port Name	Port Type
1	Win Target	VM
2	Dominion_KSX2_Port2	Not Available
3	Dominion_KSX2_Port3	Not Available
4	KSX-G2 Admin	VM
5	Dominion_KSX2_Port5	Not Available
6	Dominion_KSX2_Port6	Not Available
7	Dominion_KSX2_Port7	Not Available
8	Dominion_KSX2_Port8	Not Available
9	Cisco 2501	Serial
10	SP-2	Serial
11	Serial Port 3	Serial
12	Serial Port 4	Serial
13	SP - 5	Serial
14	Serial Port 6	Serial
15	Serial Port 7	Serial
16	Serial Port 8	Serial
17	Power Port 1 - renamed	PowerStrip
18	Power Port 2	PowerStrip

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

- Port Number. Numbered from 1 to the total number of ports available for the KSX II unit.
- Port Name. The name assigned to the port. A port name displayed in black indicates that you cannot change the name and that the port cannot be edited; port names displayed in blue can be edited.

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

- Port Type. The type of CIM connected to the port:

Port Type	Description
DCIM	Dominion CIM
Not Available	No CIM connected
VM	Virtual Media CIM (D2CIM-VUSB)

2. Click the Port Name for the port you want to edit.
  - For KVM and serial ports, the Port page will open. From this page, you can name the ports and create power associations.
  - For power strips, the Port page for power strips is opened. From this page, you can name the power strips and their outlets. name the power strips and their outlets.

---

### 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 this 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 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.

### Connect the Dominion PX

#### ➤ **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 power strip outlet.
4. Connect the power strip to an AC power source.
5. Power ON the KSX II unit.








## Port Configuration Page

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





Diagram Key	
	KSX II
	KSX II Power Ctrl. 1 Port or Power Ctrl. 2 Port
	PX
	PX Serial Port
	Cat5 Cable

## Port Configuration Page

### Assign a Name to the PX

The Port page opens when you select a port from the Port Configuration page that is connected to a Raritan remote power strip. The Type and the Name fields are pre-populated. The following information is displayed for each outlet in the power strip: outlet Number, Name, and Port Association.

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

The screenshot shows a web interface for configuring a port. At the top, there are navigation tabs: Port Access, Virtual Media, User Management, Device Settings, and Security. Below the tabs is a breadcrumb trail: Home > Device Settings > Port Configuration > Port. The main content area is titled "Port" and contains the following fields:

- Type: PowerStrip
- Name: PCR8

Below the "Port" section is an "Outlets" section with a table:

Number	Name	Port Association
1	TestPC(1)	TestPC
2	Outlet 2	
3	Outlet 3	
4	Outlet 4	
5	Outlet 5	
6	Outlet 6	
7	Outlet 7	
8	Outlet 8	

At the bottom of the form are "OK" and "Cancel" buttons.

---

*Note: When a power strip 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 power strip names containing spaces.*

---

➤ **To name the power strip (and outlets):**

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

➤ **To cancel without saving changes:**

- Click the Cancel button.

### **Associate KVM and Serial Target Servers to Outlets (Port Page)**

A server can have up to four power plugs and you can associate a different power strip with each. From 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 power strip outlets to target servers):**

---

*Note: When a power strip 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 power strip from the Power Strip Name drop-down list.
2. For that power strip, 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.

## Port Configuration Page

➤ **To cancel without saving changes:**

1. Click the Cancel button.

➤ **To remove a power strip association:**

1. Select the appropriate power strip from the Power Strip Name drop-down list.
2. For that power strip, select the appropriate outlet from the Outlet Name drop-down list.
3. From the Outlet Name drop-down list, select None.
4. Click OK. That power strip/outlet association is removed. A confirmation message is displayed.

Alternately, you can select the power strip from the Power Strip Name drop-down and then assign it a different outlet from the Outlet Name drop-down. Click OK to apply the changes. This will remove the power strips current association and associate it with the newly selected outlet. This method is not recommended by Raritan.

## Port Keywords

Port keywords work as a filter. If a keyword is detected, a corresponding message be logged in a local port log. 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

[Add](#) [Delete](#)

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:

## Port Configuration Page

- a. Click the Add button on the Port Keyword List page. The Add Keyword page will then open. Follow steps 3 - 5 to create new keywords.

Home > Device Settings > Port Keyword List > Keyword

**Add Keyword**

Keyword: ^

**Ports**

Available:		Selected:
9: Cisco 2501	<input type="button" value="Add &gt;"/>	
10: SP-2	<input type="button" value="&lt; Remove"/>	
11: Serial Port 3		
12: Serial Port 4		
13: SP - 5		
14: Serial Port 6		
15: Serial Port 7		
16: Serial Port 8		

3. Type a keyword in the Keyword field and then click on 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 on 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 on 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.

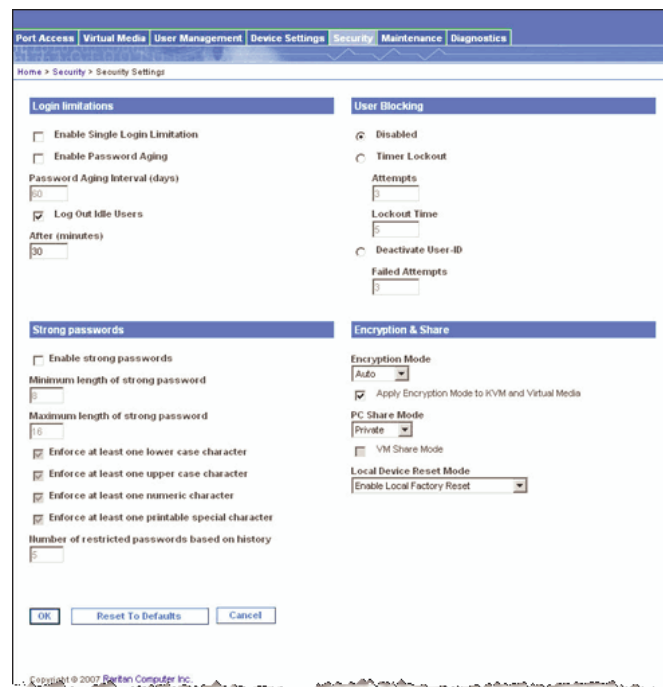
# Chapter 10 Security Settings

From the Security Settings page, you can specify login limitations, user blocking, password rules, and encryption and share.

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.



The fields are organized into the following groups: Login Limitations, Strong Passwords, User Blocking, and Encryption & Share.

2. Update the *Login Limitations* (on page 170) settings as appropriate.
3. Update the *Strong Passwords* (on page 171) settings as appropriate.
4. Update the *User Blocking* (on page 172) settings as appropriate.
5. Update the Encryption & Share settings as appropriate.



6. Click OK.
- **To close the page without saving any changes:**
  - Click Cancel.
- **To reset back to defaults:**
  - Click Reset to Defaults.

### In This Chapter

Security Settings Menu .....	169
Login Limitations .....	170
Strong Passwords .....	171
User Blocking .....	172
Encryption & Share .....	173
Checking Your Browser for AES Encryption .....	176
IP Access Control .....	176

---

## Security Settings Menu

The Security menu is organized as follows: Security Settings and IP Access Control.

Use:	To:
Security Settings	Configure security settings for login limitations, strong passwords, user blocking, and encryption & share.
IP Access Control	Control access to your KSX II unit. By setting a global access control list, you are by ensuring that your device does not respond to packets being sent from disallowed IP addresses.

---

## Login Limitations

Using Login Limitations you can specify restrictions for single login, password aging, and the logging out of idle users.

- **Enable Single Login Limitation.** When selected only one login per username is allowed at any time. When deselected, a given username/password combination can be connected into the device from several client workstations simultaneously.
- **Enable Password Aging.** When selected all users are required to change their passwords periodically, based on the number of days specified in Password Aging Interval field.
  - **Password Aging Interval (days).** This field is enabled and required when the Enable Password Aging checkbox is selected. Enter the number of days after which a password change is required. The default is 60 days.
- **Log Out Idle Users.** Select the checkbox to automatically disconnect a user session after a certain amount of inactive time has passed. Type the amount of time in the After 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.
  - **After (minutes).** 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.

## Strong Passwords

Strong passwords provide more secure local authentication for the system. Using Strong Passwords, you can specify criteria defining the format of valid KSX II local passwords such as minimum and maximum length, required characters, and password history retention.

- Enable strong passwords. Strong passwords require user-created passwords to have a minimum of 8 characters with at least one alphabetical character and one non-alphabetical character (punctuation character or number). In addition, the first four characters of the password and the username 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:
  - Minimum length of strong password. Passwords must be at least 8 characters long. The default is 8, but it can be up to 63.
  - Maximum length of strong password. The default is 16, but can be up to 64 characters long.
  - 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.

## User Blocking

- 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; the default is 5.

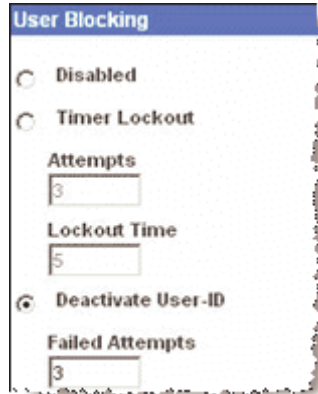
---

## 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:

- Disabled. The default option; users are not blocked regardless of the number of times they fail authentication.
- Timer Lockout. Users are denied access to the system for the specified amount of time after exceeding the specified number of unsuccessful login attempts. When selected, the following fields are enabled:
  - Attempts. The number of unsuccessful login attempts after which the user will be locked out. The valid range is 1 - 10; 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; the default is 5 minutes.

- Deactivate User-ID. When selected, this option specifies that the user will be locked out of the system after the number of failed login attempts specified in the Failed Attempts field:
  - Failed Attempts. The number of unsuccessful login attempts after which the user's User-ID will be deactivated. This field is enabled when the Deactivate User-ID option is selected. The valid range is 1 - 10.



When a user-ID is deactivated after the specified number of failed attempts, the administrator must change the user password and activate the user account by selecting the Active checkbox on the User page.

---

## 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.



## Encryption & Share

- Encryption Mode. Choose one of the options from the drop-down list. When an encryption mode is selected, a warning is displayed that if your browser does not support the selected mode, you will not be able to connect to the KSX II:

Encryption & Share

*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 Dominion KX II.*

Encryption Mode  
RC4

Apply Encryption Mode to KVM and Virtual Media

PC Share Mode  
Private

VM Share Mode

Local Device Reset Mode  
Enable Local Factory Reset

- Auto. This is the recommended option; the KSX II auto-negotiates to the highest level of encryption possible.
- RC4. 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 which provides a private communications channel between the KSX II unit and the Remote PC during initial connection authentication.
- AES-128. The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data; 128 is the key length. When AES-128 is specified, please be certain that your browser supports it, otherwise you will not be able to connect. Please refer to *Checking Your Browser for AES Encryption* (on page 176) 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, please be certain that your browser supports it, otherwise you will not be able to connect. Please refer to *Checking Your Browser for AES Encryption* (on page 176) for more information.

- 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 the selected encryption level.
- PC Share Mode. Determines global concurrent remote KVM access and serial access, enabling up to eight remote users to simultaneously log on to one KSX II and concurrently view and control the same target server through the device. Click on 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, please note that uneven control will occur if one user does not stop typing or moving the mouse.
- 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.
- Local Device Reset Mode. This option specifies which actions are taken when the hardware reset button (at the back of the unit) is depressed. For more information, refer to *Reset Button* (on page 198). Choose one of the following options:
  - Enable Local Factory Reset (Default). Returns the KSX II unit to the factory defaults.
  - Enable Local Admin Password Reset. Resets the local administrator password only. The password is reset to raritan.
  - Disable All Local Resets. No reset action is taken.

---

### Checking Your Browser for AES Encryption

If you do not know if your browser uses AES, check with the browser manufacturer, or navigate to the following website using the browser with the encryption method you want to check:

<https://www.fortify.net/sslcheck.html>. This website detects your browser's encryption method and displays a report.

Note: IE6 does not support AES 128 or 256-bit encryption.

#### **AES 256 Prerequisites and Supported Configurations**

AES 256-bit encryption is supported on the following web browsers only:

- Firefox 2.0.0.7
- Mozilla 1.7.13
- Internet Explorer 7

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 JRE's are available at the "other downloads" section of the following links:

- JRE1.4.2 - <http://java.sun.com/j2se/1.4.2/download.html>
- JRE1.5 - [http://java.sun.com/javase/downloads/index\\_jdk5.jsp](http://java.sun.com/javase/downloads/index_jdk5.jsp)

---

### IP Access Control

Using IP Access Control, you can control access to your KSX II unit. By setting a global Access Control List (ACL) you are by 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 unit as a whole, but you can also control access to your unit at the group level. Refer to *group-based IP Access Control* (see "Group-based IP ACL (Access Control List)" on page 126) 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, if 127.0.0.1 is within the range of IP Addresses that are blocked, you will not have access to the KSX II local port.**

---



➤ **To use IP Access Control:**

1. Open the IP Access Control page using one of these methods:
  - Choose Security > IP Access Control, or
  - Click the Set System ACL button from the Network Settings page

The IP Access Control page opens:

2. Select the Enable IP Access Control checkbox to enable IP access control 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 IP/Mask field.
2. Choose the Policy from the drop-down list.
3. Click Append. The rule is added to the bottom of the rules list.
4. Repeat steps 1 through 3 for each rule you want to enter.

➤ **To insert a rule:**

1. Type a Rule #. A Rule # is required when using the Insert command.

## IP Access Control

2. Type the IP Address and subnet mask in the IP/Mask 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.

➤ **To replace a rule:**

1. Specify the Rule # you want to replace.
2. Type the IP Address and subnet mask in the IP/Mask 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.

---

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

---

# Chapter 11 Maintenance

## In This Chapter

Maintenance Menu .....	179
Maintenance Features (Local/Remote Console).....	179
Audit Log .....	180
Device Information .....	181
Backup and Restore .....	182
CIM Upgrade .....	184
Firmware Upgrade.....	185
Upgrade History .....	187
Reboot.....	187

---

## Maintenance Menu

The Maintenance menu includes these options:

- Audit Log
- Device Information
- Backup/Restore
- CIM Firmware Upgrade
- Firmware Upgrade
- Factory Reset (KSX II Local Console only)
- Reboot
- Upgrade History

---

## 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.		✓

## Audit Log

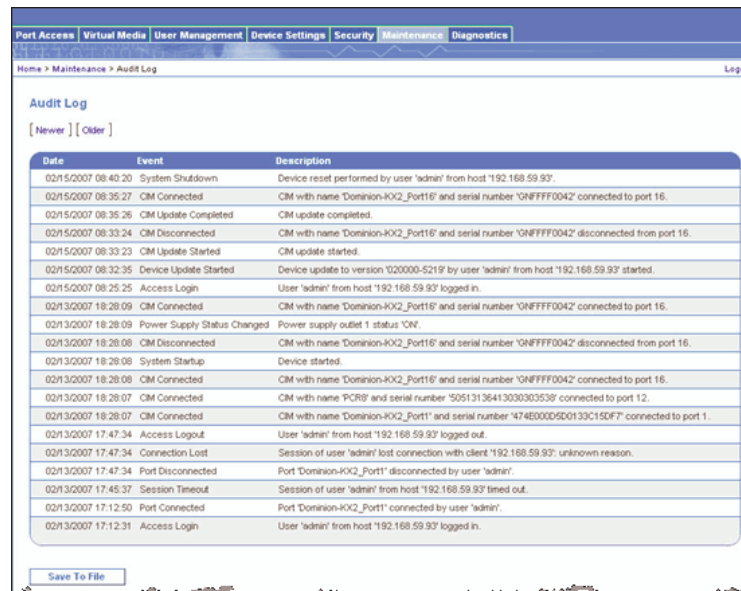
Use:	To:	Local	Remote
CIM Firmware Upgrade	Upgrade your CIMs using the firmware versions stored in the Dominion KSX II memory.	✓	✓
Firmware Upgrade	Upgrade your Dominion KSX II firmware.		✓
Factory Reset	Perform a factory reset.	✓	
Upgrade History	View information about the latest upgrade performed.	✓	✓
Reboot	Reboot the Dominion KSX II unit.	✓	✓

## Audit Log

A log is created of KSX II system events.

➤ **To view the audit log for your KSX II unit:**

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; 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 the Save to File button. A Save File dialog box opens.
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 KSX II and CIMs:**

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

The screenshot shows a web browser window with the following content:

Home > Maintenance > Device Information Logout

**Device Information**

**Model:** DKSX2\_188  
**Hardware Revision:** 0x60  
**Firmware Version:** 1.0.0.2.6178  
**Serial Number:** HKD9600001  
**MAC Address:** 00:0d:5d:03:5d:04

**CIM Information**

Port	Name	Type	Firmware Version	Serial Number
1	Win Target	VM	2A45	HJW7250865
4	KSX-G2 Admin	VM	2A45	HJW7250866

## Backup and Restore

The following information is provided about the KSX II: Model, Hardware Revision, Firmware Version, Serial Number, and MAC Address.

The following information is provided about the CIMs in use: Port (number), Name, Type (of CIM: DCIM, Power Strip, or VM), Firmware Version, and Serial Number.

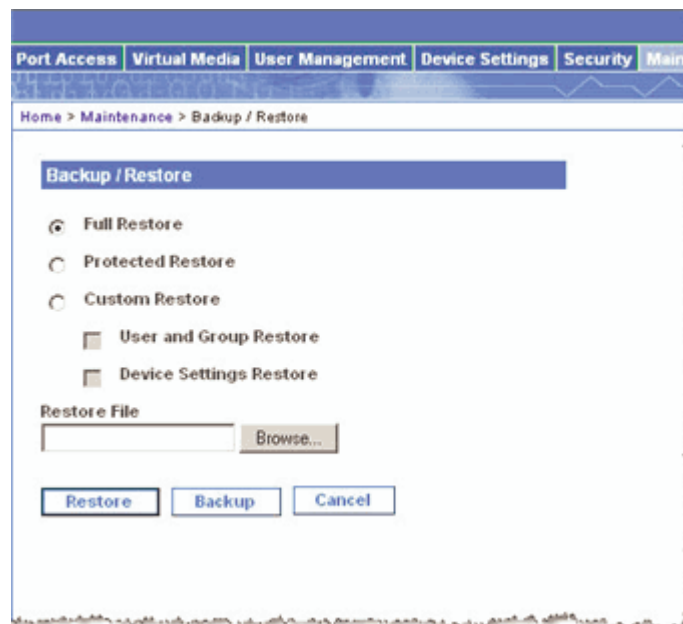
---

## 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 setup 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 a web interface for the Backup / Restore page. At the top, there is a navigation menu with tabs: Port Access, Virtual Media, User Management, Device Settings, Security, and Maintenance. Below the menu, the breadcrumb path is Home > Maintenance > Backup / Restore. The main content area is titled "Backup / Restore" and contains the following options:

- Full Restore
- Protected Restore
- Custom Restore
  - User and Group Restore
  - 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 three buttons: "Restore", "Backup", and "Cancel".

---

*Note: Backups are always complete system backups. Restores can be complete or partial depending on your selection.*

---

➤ **To backup your KSX II:**

1. Click Backup. A File Download dialog opens.
2. Click Save. A Save As dialog opens.
3. Choose the location, specify a file name, and click Save. A Download Complete dialog opens.
4. Click Close. The backup file is saved locally on your client machine with the name and location specified.

➤ **To restore your KSX II:**

WARNING: Please 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 serial number, MAC Address, IP Address, name, etc. 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. Select the appropriate checkboxes:

## CIM Upgrade

- User and Group Restore. This option includes only user and group information. Use this option to quickly set up users on a different KSX II.
  - Device Settings Restore. This option includes only device settings. Use this option to quickly copy the device information.
2. Click the Browse button. A Choose File dialog opens.
  3. Navigate to and select the appropriate backup file and click Open. The file selected is listed in the Restore File field.
  4. Click Restore. The configuration (based on the type of restore selected) is restored.

---

## CIM Upgrade

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

---

*Note: Only D2CIM-VUSB can be upgraded from this page.*

---

➤ **To upgrade CIMs using the KSX II memory:**

1. Choose Maintenance > CIM Firmware Upgrade. The CIM Upgrade from KSX II Flash page opens.
2. The Port (number), Name, Type, Current CIM Version, and Upgrade CIM Version are displayed for easy identification of the CIMs.
3. Select the Selected checkbox for each CIM you want to upgrade.

---

Tip: Use the Select All and Deselect All buttons to quickly select all (or deselect all) of the CIMs.

---

4. Click the Upgrade button. You are prompted to confirm the upgrade.
5. Click OK to continue the upgrade. Progress bars are displayed during the upgrade. Upgrading takes approximately 2 minutes (or less) per CIM.



- **To exit without upgrading:**
  - Click Cancel.

**CIM Upgrade from Device Flash**

*KsX2 CIMs:*

Selected	4 Port	Name	Type	Current CIM Version	Upgrade CIM Version
<input type="checkbox"/>	1	Win Target1	VM	2A46	2A46
<input type="checkbox"/>	4	KSX-G2 Admin	VM	2A46	2A46

---

## Firmware Upgrade

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

---

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

---

- **To upgrade your KSX II unit:**
  1. Locate the appropriate Raritan firmware distribution file (\*.RFP), found on the Raritan Firmware Upgrades Web page: <http://www.raritan.com/support/firmwareupgrades> and download the file.
  2. Unzip the file. Please read all instructions included in the firmware ZIP files carefully before upgrading.

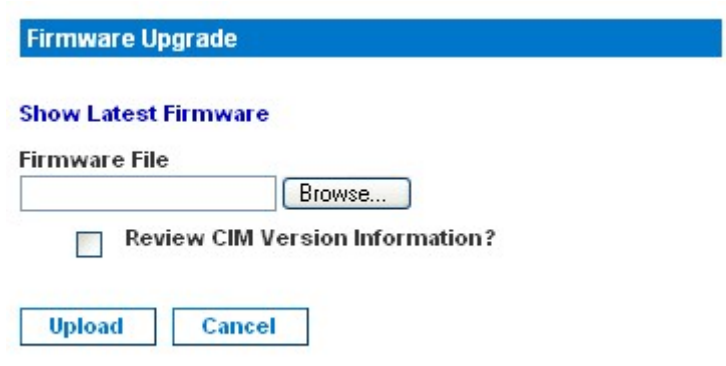
---

Note: Copy the firmware update file to a local PC before uploading. Do not load the file from a network drive.

---

## Firmware Upgrade

3. Choose Maintenance > Firmware Upgrade. The Firmware Upgrade page opens.



**Firmware Upgrade**

**Show Latest Firmware**

**Firmware File**

**Review CIM Version Information?**

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

---

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

---

7. Click Upgrade. Please wait for the upgrade to complete. Status information and progress bars are displayed during the upgrade. Upon completion of the upgrade, the unit reboots (1 beep sounds to signal the reboot).
8. As prompted, close the browser and wait approximately 5 minutes before logging in to the KSX II again.

## Upgrade History

KSX II provides information about upgrades performed on the KSX II unit 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 last KSX II upgrade that was run, the final status of that upgrade, and the firmware version. Information is also provided about the CIMs:

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

## Reboot

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

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

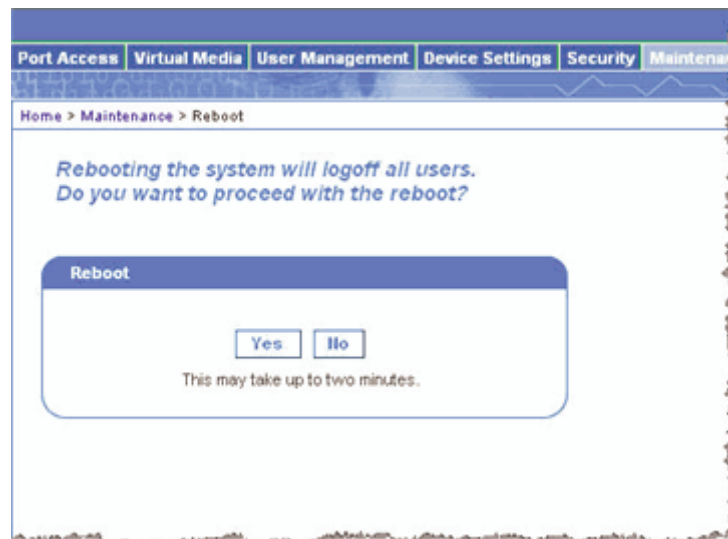
## Reboot

### ➤ **To reboot your KSX II:**

1. Choose Maintenance > Reboot. The Reboot page opens:



2. Click the Reboot button. You are prompted to confirm the action:



3. Click Yes to proceed with the reboot.

### ➤ **To exit without rebooting:**

- Click No.

# Chapter 12 Diagnostics

## In This Chapter

Diagnostics Menu .....	189
Network Interface Page.....	190
Network Statistics Page.....	190
Ping Host Page.....	193
Trace Route to Host Page .....	194
Device Diagnostics.....	195

---

## Diagnostics Menu

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; the information displayed is the output of those commands.

The following Diagnostics menu options help you debug and configure the network settings:

- Network Interface
- Network Statistics
- Ping Host
- Trace Route to Host

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

Use:	To:
Network Interface	Obtain the status of network interface.
Network Statistics	Obtain statistics about the network.
Ping Host	Determine whether a particular host is reachable across an IP network.
Trace Route to Host	Determine the route taken all the way to the selected host.
Device Diagnostics	Use when directed by Raritan Technical Support (Remote Console only).

---

## 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 ping-able or not.
  - The LAN port that is currently active.
- **To refresh this information:**
    - Click the Refresh button.

---

## Network Statistics Page

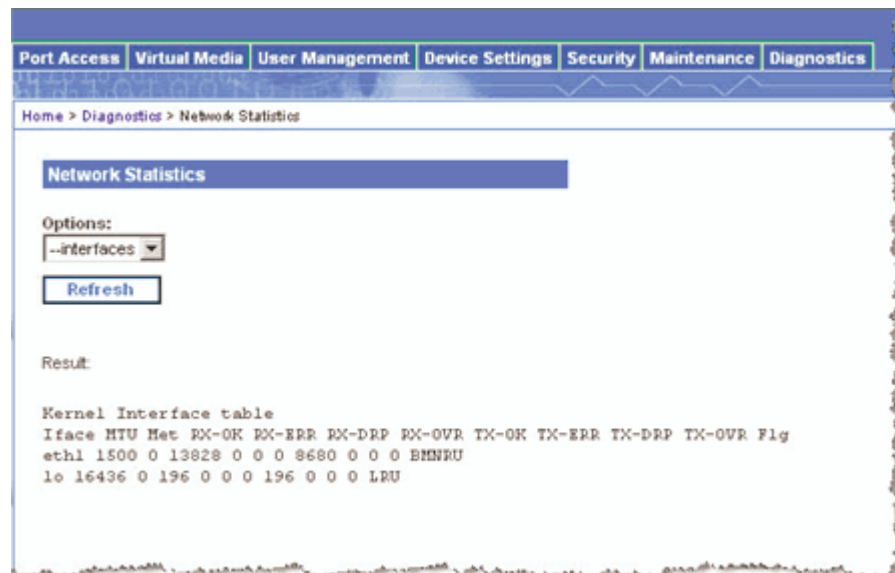
The KSX II provides statistics about your network interface.

- **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:

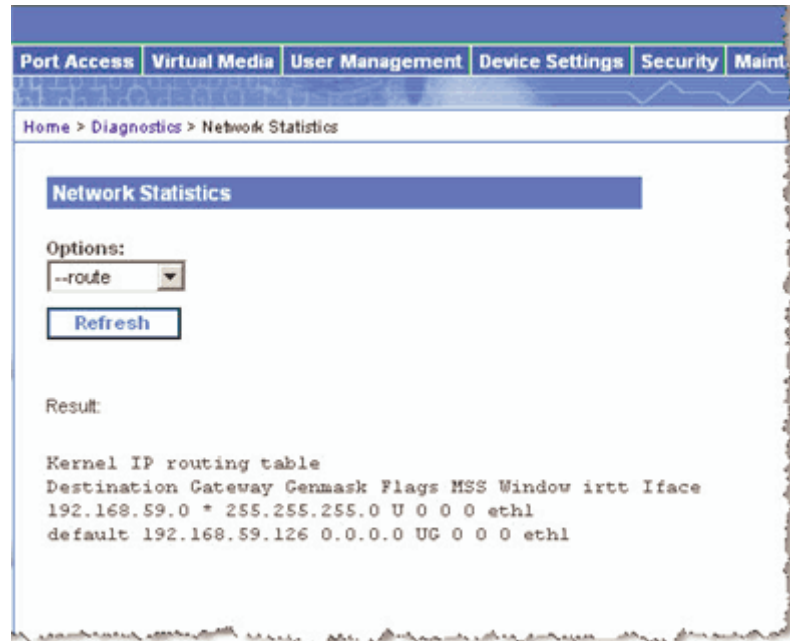


- Interfaces. Produces a page similar to the one displayed here:



## Network Statistics Page

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



3. Click the Refresh button.

The relevant information is displayed in the Result field.



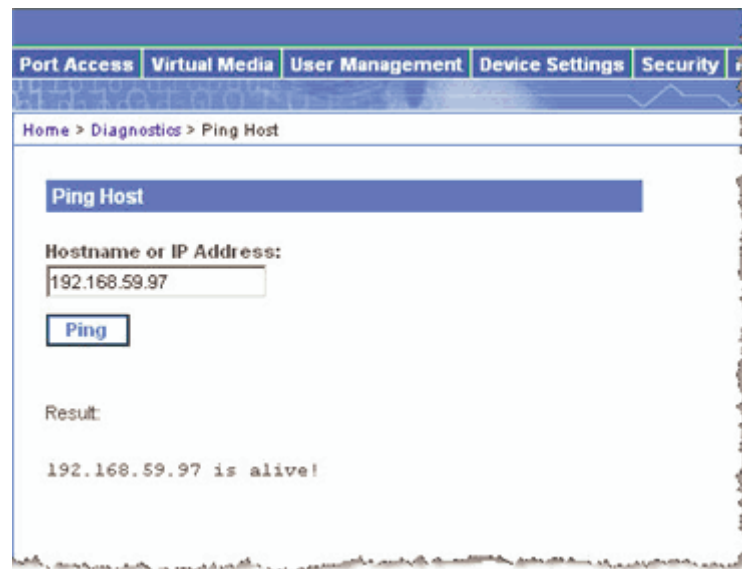
---

## 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 unit is accessible.

➤ **To ping the host:**

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



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.

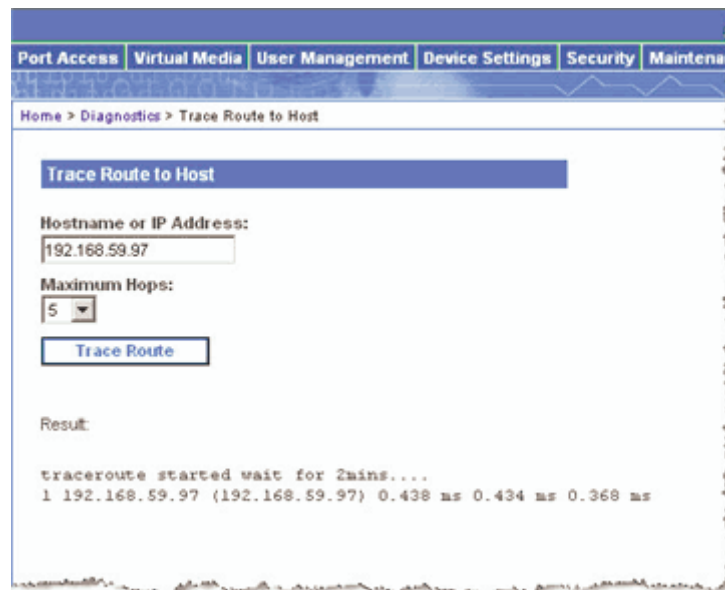
---

### Trace Route to Host Page

Trace Route is a network tool used to determine the route taken all the way 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:



Port Access Virtual Media User Management Device Settings Security Maintenance

Home > Diagnostics > Trace Route to Host

**Trace Route to Host**

Hostname or IP Address:

Maximum Hops:

Result:

```
traceroute started wait for 2mins...  
1 192.168.59.97 (192.168.59.97) 0.438 ms 0.434 ms 0.368 ms
```

2. Type either the Hostname or IP Address into the Hostname or IP Address field.
3. Choose the Maximum Hops from the drop-down list (5 to 50 in increments of 5).
4. Click the Trace Route button. 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.

---

## 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:

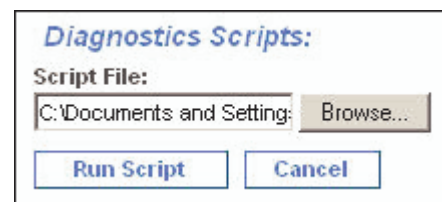
- **Diagnostics Scripts.** Execute a special script provided by Raritan Technical Support during a critical error debugging session. The script is uploaded to the unit and executed. Once this script has been executed, you can download the diagnostics messages through the Save to File button.
  - **Device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

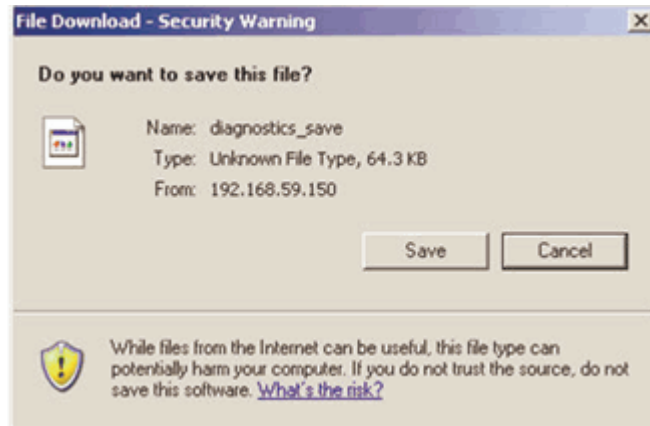
1. Choose Diagnostics > Device Diagnostics. The Device Diagnostics page opens.
2. To execute a diagnostics script file emailed to you from Raritan Technical Support:
  - a. Retrieve the diagnostics file supplied by Raritan and unzip as necessary.
  - b. Use the Browse button. A Choose File dialog box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



- e. Click Run Script.
  - f. Sent this file to Raritan Technical Support using step 4.
3. To create a diagnostics file to send to Raritan Technical Support:

## Device Diagnostics

- a. Click the Save to File button. The File Download dialog opens:



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

# Chapter 13 KSX II Local Console

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.

The KSX II Local Console supports the following language keyboards: US English, UK English, German, French, Japanese, Korean, Simplified Chinese, and Traditional Chinese.

---

*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.*

---

## In This Chapter

Reset Button .....	198
Physical Connections .....	198
Starting the KSX II Local Console .....	199
Server Display .....	200
Hotkeys.....	201
Accessing a Target Server.....	201
Returning to the KSX II Local Console Interface .....	202
Local Port Administration.....	202

## Reset Button

---

### Reset Button

At the back of the KSX II unit, there is a Reset button. It is recessed to prevent accidental presses (you will need a pointed object to use this button).

The actions that are performed when the reset button is pressed are defined in the graphical user interface. Refer to Security Settings, Encryption & Share for more information.

---

*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, please refer to **Audit Log** (on page 180).*

---

➤ **To reset the unit:**

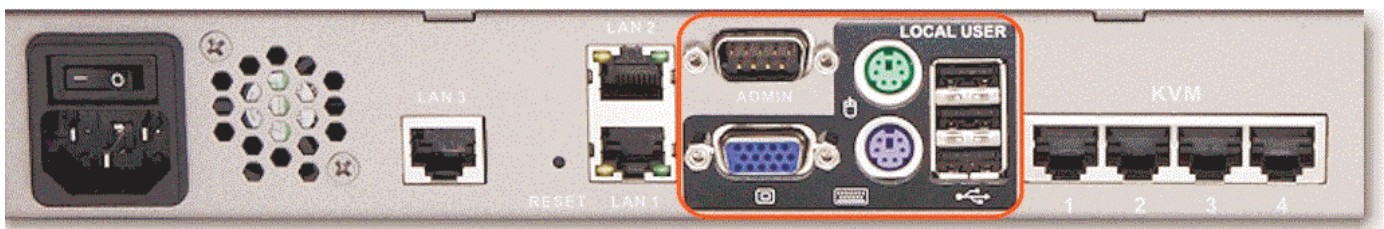
1. Power off the KSX II unit.
2. Use a pointed object to press and hold the reset button.
3. While continuing to hold the reset button, power the KSX II unit back on.
4. Continue holding the reset button for 5-10 seconds. Once the unit has been reset; two short beeps signal completion.



---

### Physical Connections

The physical connections for the local ports can be found on the back panel of the KSX II:



Monitor: Attach a standard multi-sync VGA monitor to the HD15 (female) video port.

Keyboard: Attach either a standard PS/2 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 PS/2 mouse to the Mini-DIN6 (female) mouse port or a standard USB mouse to one of the USB Type A (female) ports.

---

## Starting 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.

---

### Security and Authentication

In order to use the KSX II Local Console, you must first authenticate with a valid username and password. KSX II provides a fully-integrated authentication and security scheme, whether your access is via the network or the local port. In either case, KSX II allows access only to those servers to which a user has access permissions (refer to 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. You need a keyboard, mouse, and video display connected to the local ports at the back of the KSX II unit. Refer to Physical Connections for more information about the local port connections.
2. Start the KSX II unit; the KSX II Local Console interface displays.

## Server Display

---

### KSX II Local Console Interface

The KSX II Local Console interface is almost identical to the KSX II Remote Console interface. Where there are differences, they are noted in the user manual. Refer to User Interfaces, *Console* (see "KSX II Local Console: KSX II Devices" on page 55), and Console Menu Tree for additional information.

---

### 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.

---

## 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, the connected 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 unit. Please note that ports connected to power strips will not be among those listed.
- Port Name. The name of the KSX II port; initially set to Dominion-KSX II-Port#, but you can change the name to something more descriptive. When you click on the Port Name link, an Action Menu is opened. Refer to the Port Action Menu for more information about the menu options available.

---

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

---

- Status. The Status is either up or down.
- Availability. Valid Values per include Idle, Connected, Busy, or Unavailable.

➤ **To change the sort order:**

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

---

## Hotkeys

Because the KSX II Local Console interface is completely replaced by the interface for the target server you are accessing, a hotkey is utilized so you can switch between these interfaces.

The Local Port hotkey allows you to rapidly access the KSX II Local Console user interface when a target server is currently being viewed. The default is to press the Scroll Lock key twice in rapid succession, but you can designate another key combination (available in the Local Port Settings page) as the hotkey. Refer to *Local Port Settings* (see "Local Port Settings (KSX II Local Console Only)" on page 203) for more information.

---

## 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.

---

## **Returning to the KSX II Local Console Interface**

---

**Important:** The KSX II Local Console default hotkey is to press the Scroll Lock key twice rapidly. This key combination can be changed in the *Local Port Settings* (see "Local Port Settings (KSX II Local Console Only)" on page 203) page.

---

- **To return to the KSX II Local Console from the target server:**
  - Press the hotkey (default is Scroll Lock) twice rapidly. 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. Please note that the KSX II Local Console also provides access to these administrative functions:

- Local Port Settings
- Factory Reset

---

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

---

---

### Local Port Settings (KSX II Local Console Only)

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

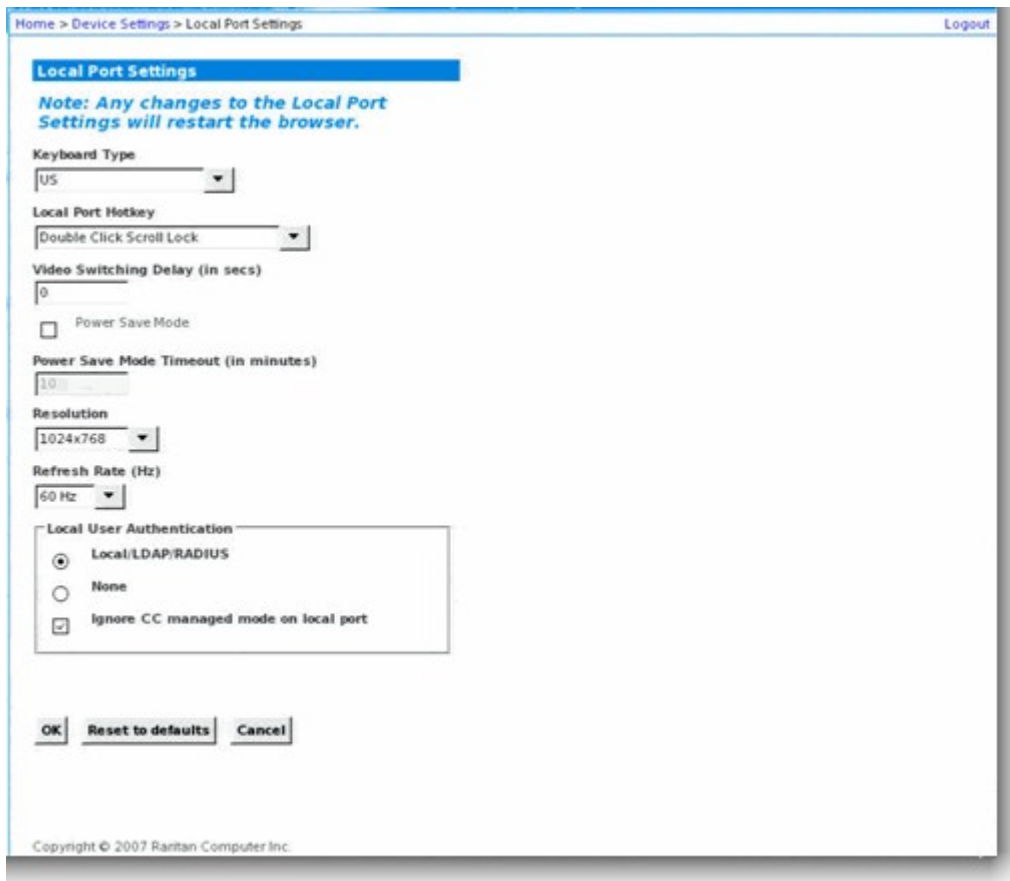
---

*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
  - UK

## Local Port Administration

- French
  - German
  - JIS (Japanese Industry Standard)
  - Simplified Chinese
  - Traditional Chinese
  - Dubeolsik Hangul (Korean)
  - German
  - Norwegian
  - Swedish
  - Danish
  - Belgian
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 Double Click Scroll Lock, but you can select any key combination from the drop-down list:

Hotkey:	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 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/LDAPS/RADIUS. This is the recommended option; for more information about authentication, refer to *Remote Authentication* (on page 48) and Authentication vs. Authorization.
    - 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 clear this checkbox but then want local port access, you will have to remove the device from under CC-SG management (from within CC-SG) and then you will be able to check this checkbox.

---

10. Click OK.

➤ **To close the page without saving any changes:**

- Click Cancel.

➤ **To reset back to defaults:**

- Click Reset to Defaults.

---

### Factory Reset (KSX II Local Console Only)

---

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

---

The KSX II offers several types of reset modes from the Local Console user interface.

---

*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, please refer to **Audit Log** (on page 180).*

---

➤ **To perform a factory reset:**

1. Choose Maintenance > Factory Reset. The Factory Reset page opens.
2. Choose the appropriate reset option.
  - Full Factory Reset: Removes the entire configuration and resets the unit completely to the factory defaults. Please 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 (from Device Settings > Network Settings) of the unit back to the default values:
    - 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)

You will be prompted to confirm this action because all network settings will be permanently lost.

1. Click Reset to continue. You will be prompted to confirm the factory reset.

2. Click the Really Reset button to proceed. Upon completion, the KSX II unit is automatically restarted.

# Chapter 14 Raritan Serial Console

The standalone Raritan Serial Console (RSC) is used to make direct connections to the serial target without going through the KSX II Local Client application. You specify the KSX II address and the port number (target) and are connected.

## In This Chapter

System Requirements .....	208
Installing RSC on Windows .....	213
Installing RSC for Sun Solaris and Linux .....	215
Launching RSC from a KSX II Remote Console.....	216
Raritan Serial Client Interface .....	217

---

## System Requirements

The following requirements must be met to support the Raritan Serial Console:

- The RSC will function with JRE version 1.4.2\_05 or later (except for JRE version 1.5.0\_02). However, for optimum performance, Raritan recommends using JRE 1.5.0 (except, of course for 1.5.0\_02).
- Your system may require configuration adjustments depending on the operating system and browser. The JRE provides configuration instructions with the JRE download. Browse to the page at <http://www.java.com/en/download/help/testvm.xml> (http://www.java.com/en/download/help/testvm.xml \o http://www.java.com/en/download/help/testvm.xml) to determine the JRE version currently installed on your system. If you do not have a compatible version of the JRE, go to <http://www.java.com> (http://www.java.com) and click the Download Now button.

---

*Note: Raritan does not support JRE version 1.5.0\_02 for use with the RSC.*

---

- Minimum 1 GHz PC with 512 MB RAM.

Ensure that Java can be started from the command line. To do this, environment variables must be configured. Make a note of the exact path where Java was installed. (The path information will be used later.)

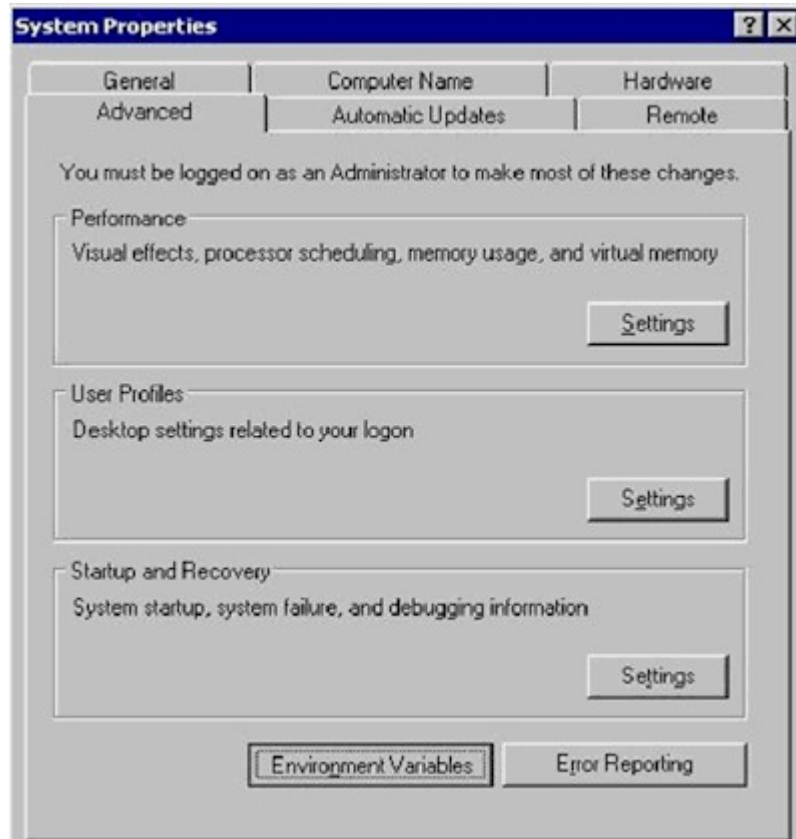
---

### Setting Windows OS Variables

1. Open the Start menu, and then open the Control Panel and choose System.



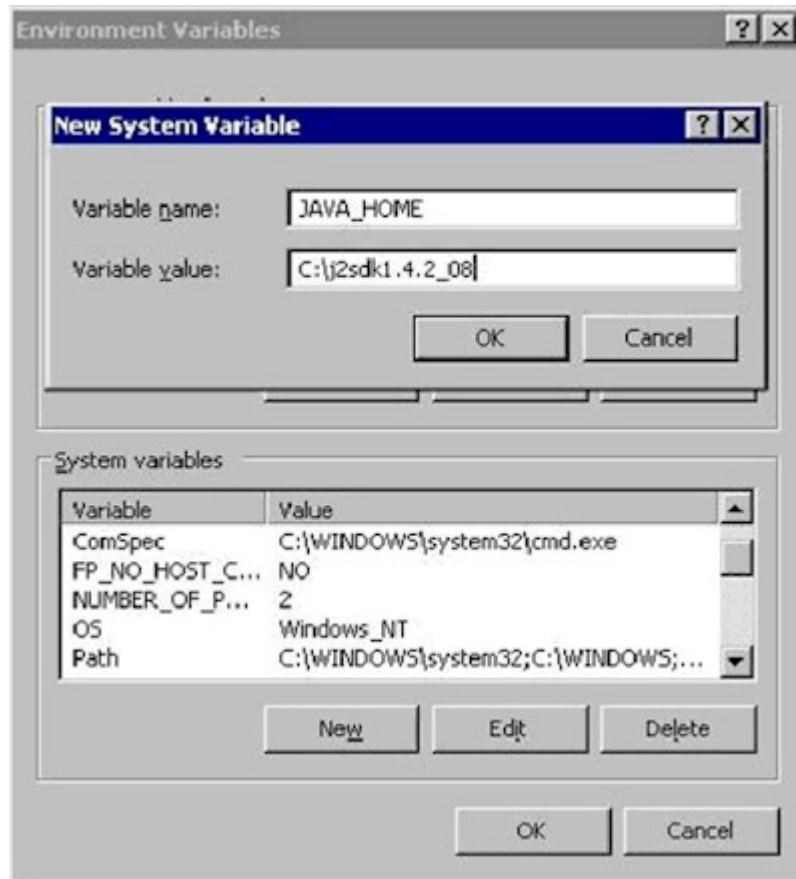
2. Go to Advanced and open Environment Variables.



3. In the System variables section, click New.
4. In the New System Variable dialog, add JAVA\_HOME to the Variable name block and the path you wrote down earlier in the Variable value block.

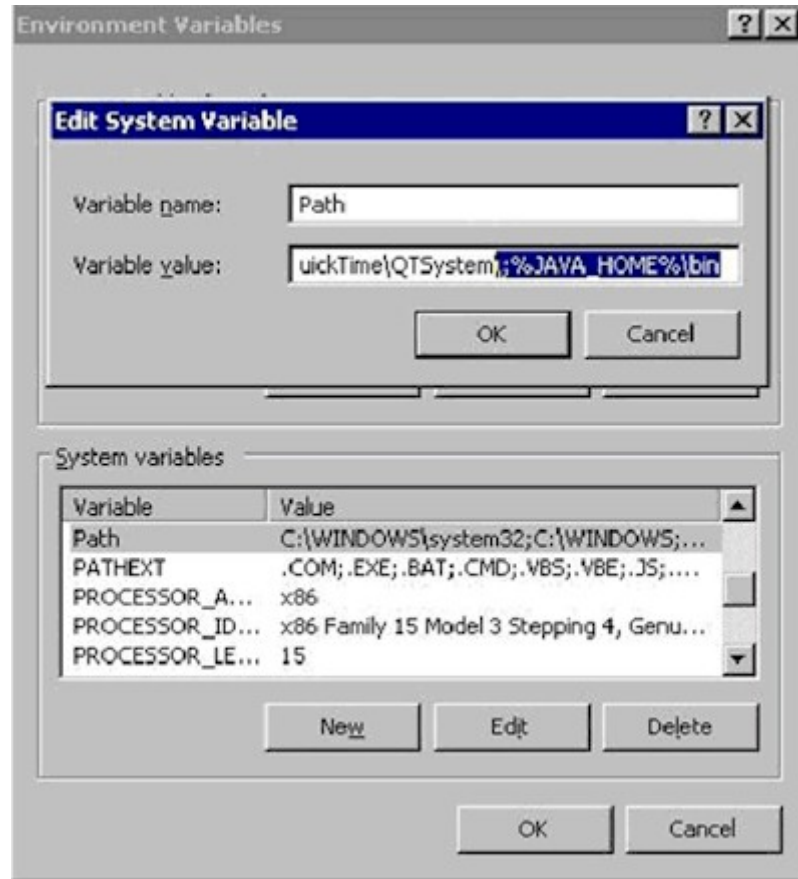
## System Requirements

5. Click OK.



6. Select the PATH variable and click Edit.
7. Add %JAVA\_HOME%\bin to the end of the current Variable value. Ensure a semicolon (;) separates the new value from the last value in the string.

- 8. Click OK.



- 9. Select the CLASSPATH variable and click Edit.
- 10. Ensure the CLASSPATH Variable value is configured properly; that is, its value must have a period (.) in it. If, for any reason, there is no CLASSPATH variable defined, create one.



---

### Setting Linux OS Variables

If you want to set Java for this user only, open and edit `.profile` file located in the `/home/Username` folder.

If you want to set Java for all users, open `.profile` file in your `/etc` folder:

1. Find the line where you set your PATH

Example: `export PATH=$PATH:/home/username/somefolder`

2. Before that line you must set your JAVA\_HOME and then modify your PATH to include it.

To achieve this, add the following lines:

```
export
JAVA_HOME=/home/username/j2sdk1.4.2/
export PATH=$PATH:$JAVA_HOME/bin
```

3. Save the file and you are finished.

---

### Setting UNIX OS Variables

Perform the following steps to check the latest JRE Version on Sun Solaris.

1. Launch a terminal window on the Sun Solaris desktop.
2. Type `java -version` in the command line and press ENTER. The currently-installed version of Java Runtime Environment (JRE) appears.

- If your path variable is not set to where the java binaries have been installed, you may not be able to see the JRE version.

- To set your path: Assuming JRE 1.4.2\_05 is installed in `/usr/local/java`: you must set your PATH variable.

- To set path for bash shell:

```
export
PATH=$PATH:/usr/local/java/j2re1.4.2_05/bin
```

- To set path for tcsh or csh:

```
set PATH = ($PATH
/usr/local/java/j2re1.4.2_05/bin)
```

- These commands can either be typed at the terminal each time you log in, or you can add them to your `.bashrc` for bash shell or `.cshrc` for csh or tcsh so that each time you log in, the PATH is already set. See your shell documentation if you encounter problems.



```
# java -version
java version "1.4.2_05"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2_05-b04)
Java HotSpot(TM) Client VM (build 1.4.2_05-b04, mixed mode)
#
```

3. If the JRE is version 1.4.2\_05 or later, but not version 1.5.0\_02, proceed with the RSC installation. If the version is older, go to the Sun website at: <http://java.sun.com/products/> (<http://java.sun.com/products/>) to download the latest Runtime Environment.

---

## Installing RSC on Windows

You must have administrative privileges to install RSC.

➤ **To install RSC on Windows:**

1. Log on to a Windows machine.
2. Download, or copy from a known location, the RSC-installer.jar installation file.
3. Double-click on the executable file to start the installer program. The splash screen appears.
4. Click Next. The installation path screen appears.
5. Change the path, if desired.
6. Click Next. The installation progress screen appears.

## Installing RSC on Windows

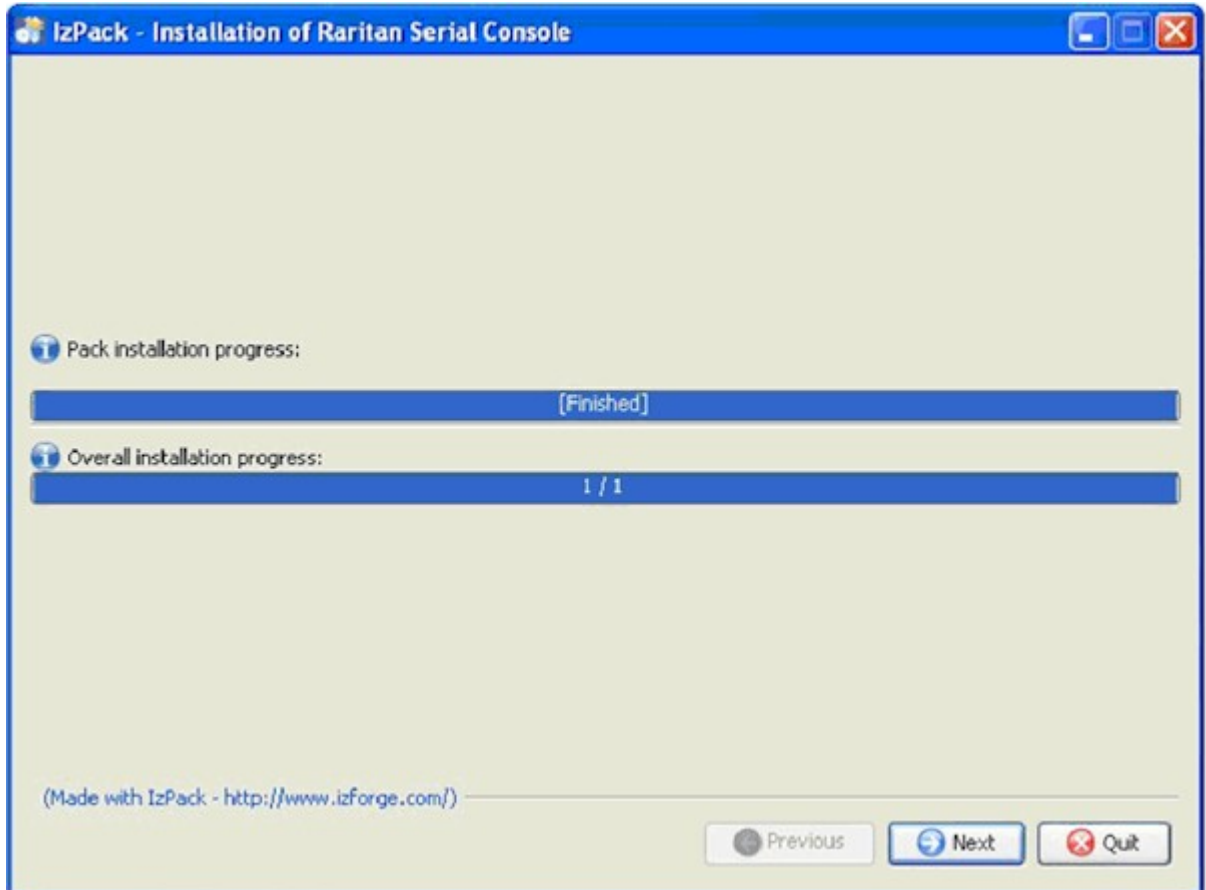
---

Note: The standalone version of Raritan Serial Console (RSC) is available from the Raritan Support website:

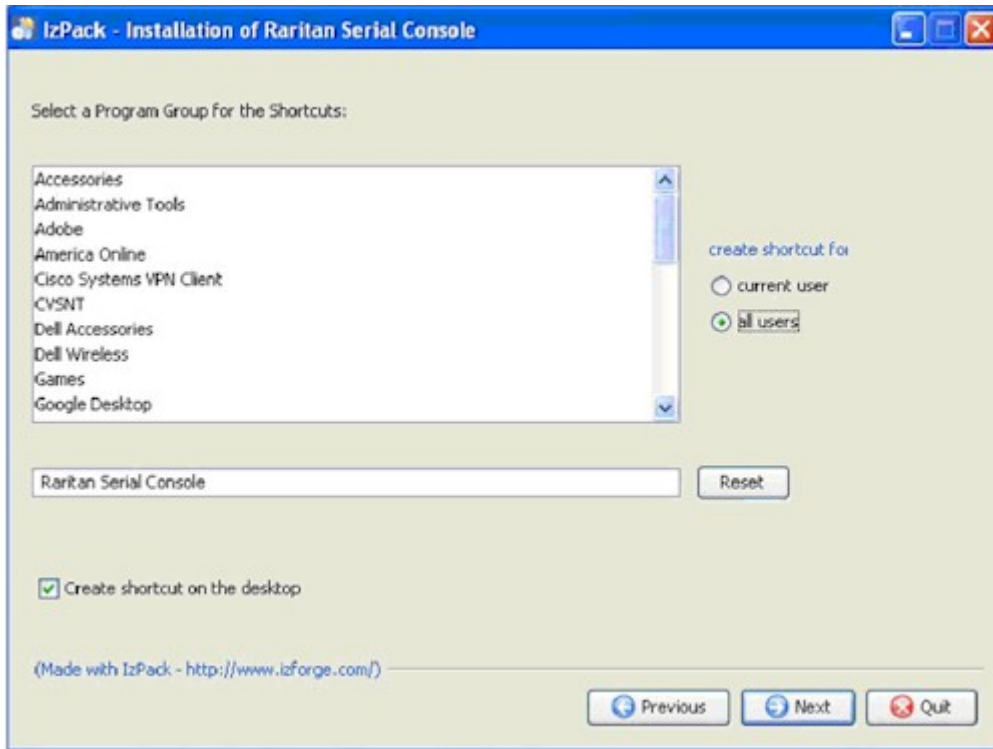
[http://www.raritan.com/support/sup\\_upgrades.aspx](http://www.raritan.com/support/sup_upgrades.aspx)

([http://www.raritan.com/support/sup\\_upgrades.aspx](http://www.raritan.com/support/sup_upgrades.aspx))

---



7. Click Next. The Windows shortcut screen appears.



8. Specify the desired Program Group for the Shortcut.
9. Click Next. The installation finished screen appears.
10. Click Done.

---

## Installing RSC for Sun Solaris and Linux

You must have administrative privileges to install RSC.

1. Log on to your Sun Solaris machine.
2. Download, or copy from a known location, the RSC-installer.jar installation file.
3. Open a terminal window and change to the directory where the installer is saved.
4. Type `java -jar RSC-installer.jar` and press ENTER to run the installer.
5. Click Next after the initial screen loads.
6. The Set Installation Path screen appears.
  - a. Select the directory where you want to install RSC and click Next.

## Launching RSC from a KSX II Remote Console

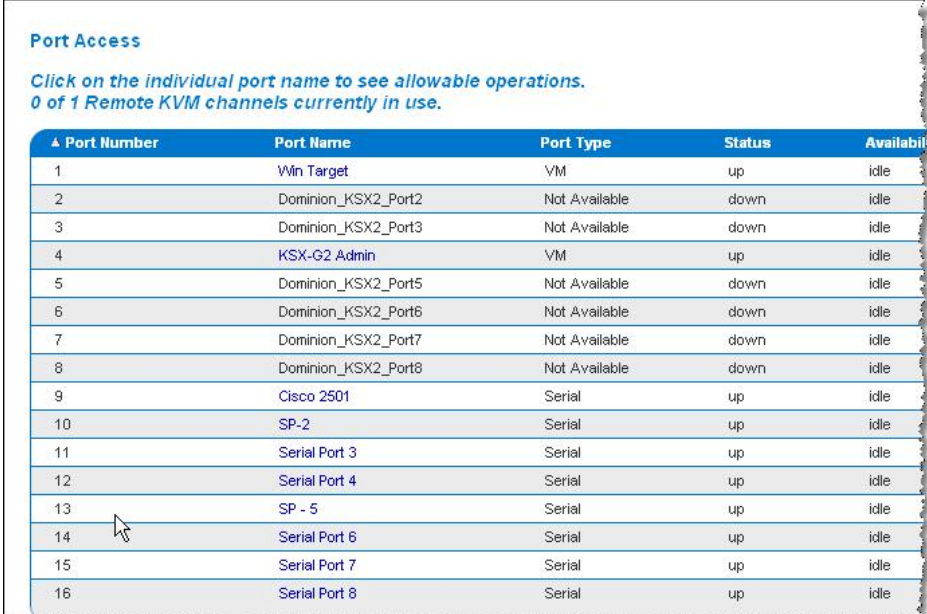
- b. Click Browse to navigate to a non-default directory.
- c. Click Next when the installation is complete.
- d. Click Next again. The installation is complete. The final screen indicates where you will find an uninstaller program, and allows the option of generating an automatic installation script.
- e. Click Done to close the Installation window.

---

## Launching RSC from a KSX II Remote Console

➤ **To launch 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	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

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

---

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

---



The Raritan Serial Console window appears. For information, see to *Raritan Serial Console Interface* (see "Raritan Serial Client Interface" on page 217) section in this chapter.

---

Note: You can download the standalone Raritan Serial Client from the Raritan support website: <http://www.raritan.com/support> (<http://www.raritan.com/support>).

---

➤ **To launch RSC from the Windows desktop:**

1. Double-click on the shortcut or use Start Programs to launch the standalone RSC. The Raritan Serial Console Login connection properties window appears.
2. Enter the Dominion KSX II IP address, account information, and the desired target (port).
3. Click Start. The RSC opens with a connection to the port.

---

Note: In case of unrecognized characters or blurry screens that might appear in RSC window due to localization support, please try changing the font to Courier New. Go to: Emulator à Settings à Display, and select Courier New for Terminal Font Properties or GUI Font Properties.

---

*Note: When RSC connects 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 launch 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 launch RSC.
3. Double-click on the desired device to establish a connection.
4. Type your Username and Password.
5. Click OK to log on.

---

## Raritan Serial Client Interface

---

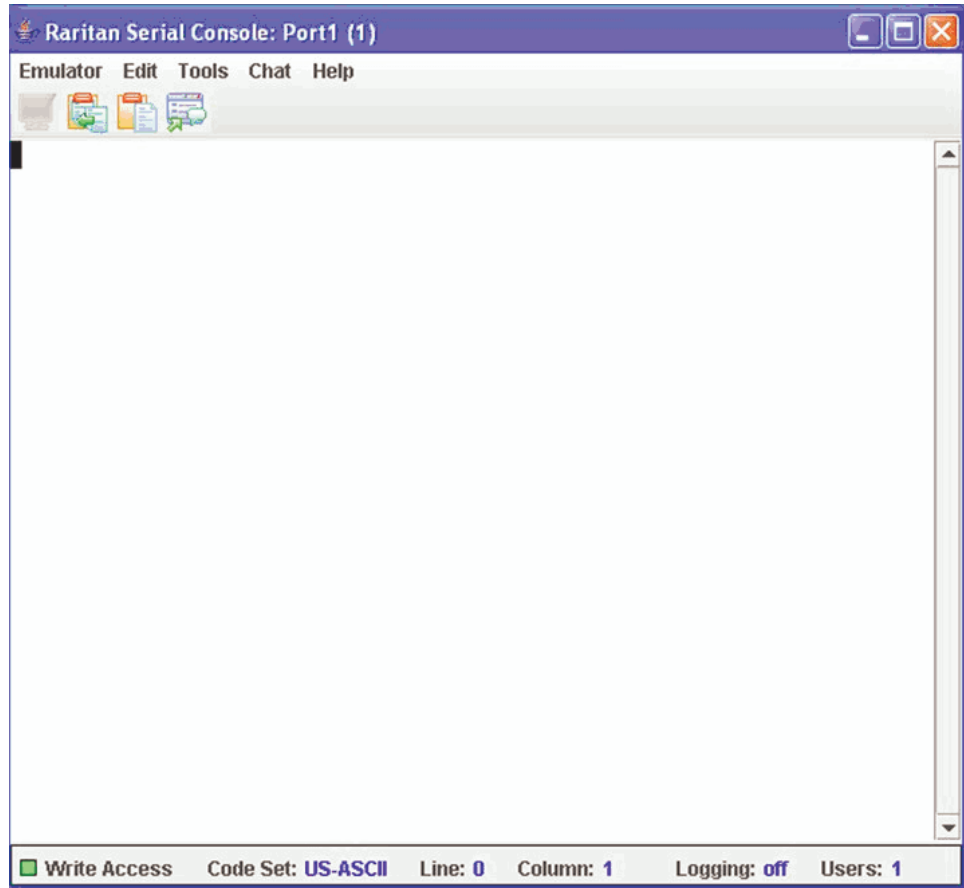
**Important:** The Raritan Serial Console screen usually opens in a separate window in back of the Port page. With some versions of Java on Windows, the screen opens in front of the Port screen.

---

## Raritan Serial Client Interface

Minimize the Port Access page to access the Raritan Serial Console screen. The RSC contains drop-down menus that provide the user with the ability to:

- Modify emulation settings such as fonts and window size.
- Manage the history of the session.
- Request Write Access to the port.
- Get a Write Lock on the port.
- Send a Break signal (used for Solaris servers).
- Get a list of users connected to this port.
- Edit text in the window.
- Manage client workstation-based logging of data from the target device.
- Send Keystroke (combinations).
- Send Text files.
- Send power commands to a Power Distribution Unit (PDU).
- Chat among other users on the same port.
- Get help.



---

### Default RSC Option Values

The following default values apply to the GUI font properties, colors and fonts defined in RSC:

Item	Value
Font Properties	Monospaced
GUI Font Properties	Monospaced
Colors	Black Foreground and White Background

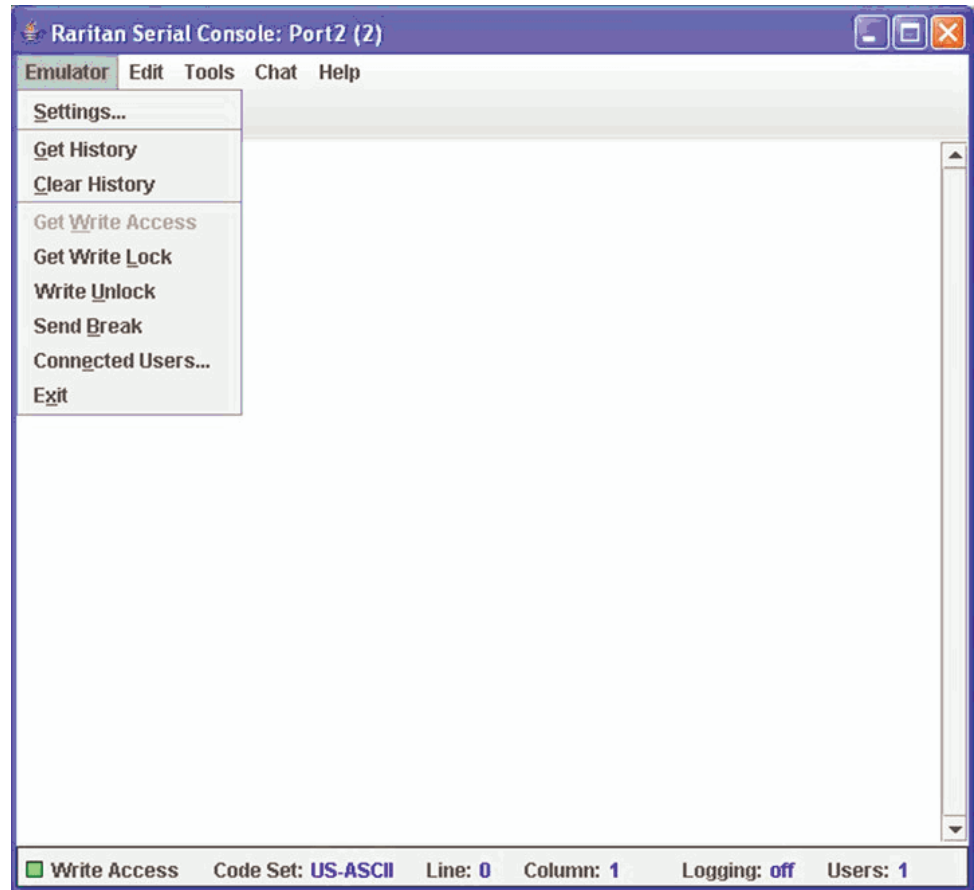
---

### Emulator

1. Change the default user Idle Timeout setting before launching the RSC for the first time or it will timeout in 10 minutes and display a host termination message. See the Security section of the KSX II User Guide for changing the Idle Timeout setting..

## Raritan Serial Client Interface

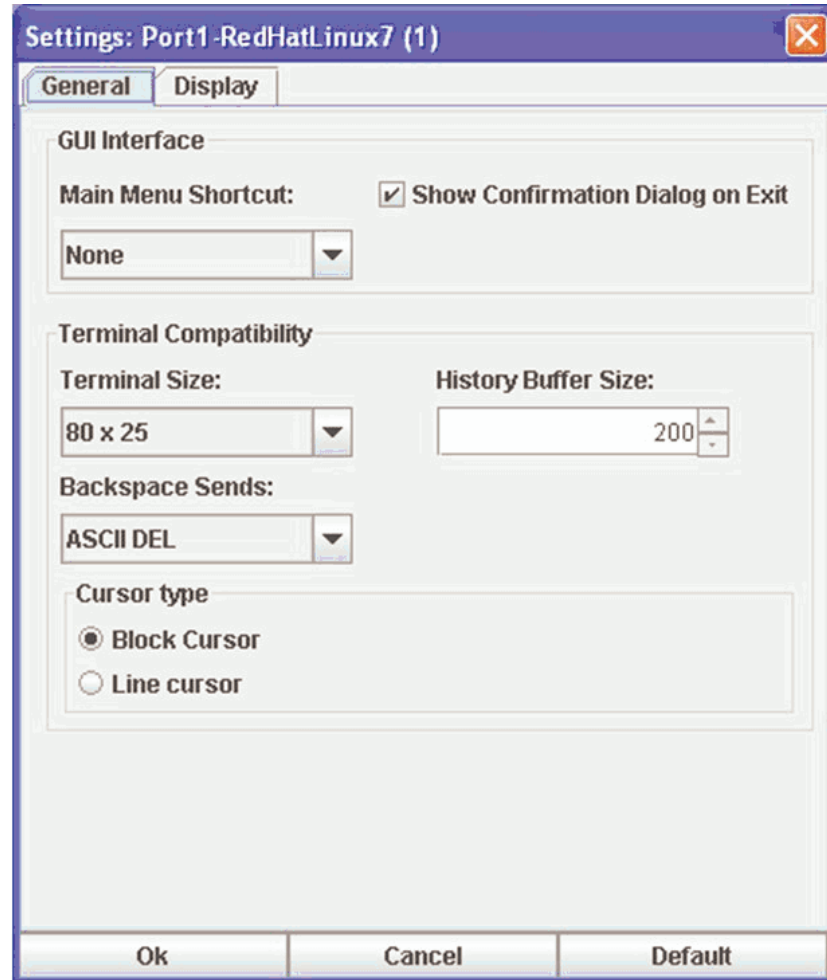
2. Click the Emulator drop-down menu to display a list of topics.



**Settings**

*Note: Terminal emulation settings are set with the port by an Administrator using the Setup->Port Configuration menu.*

1. Choose Emulator > Settings. The Settings screen displays the General tab with the default settings.



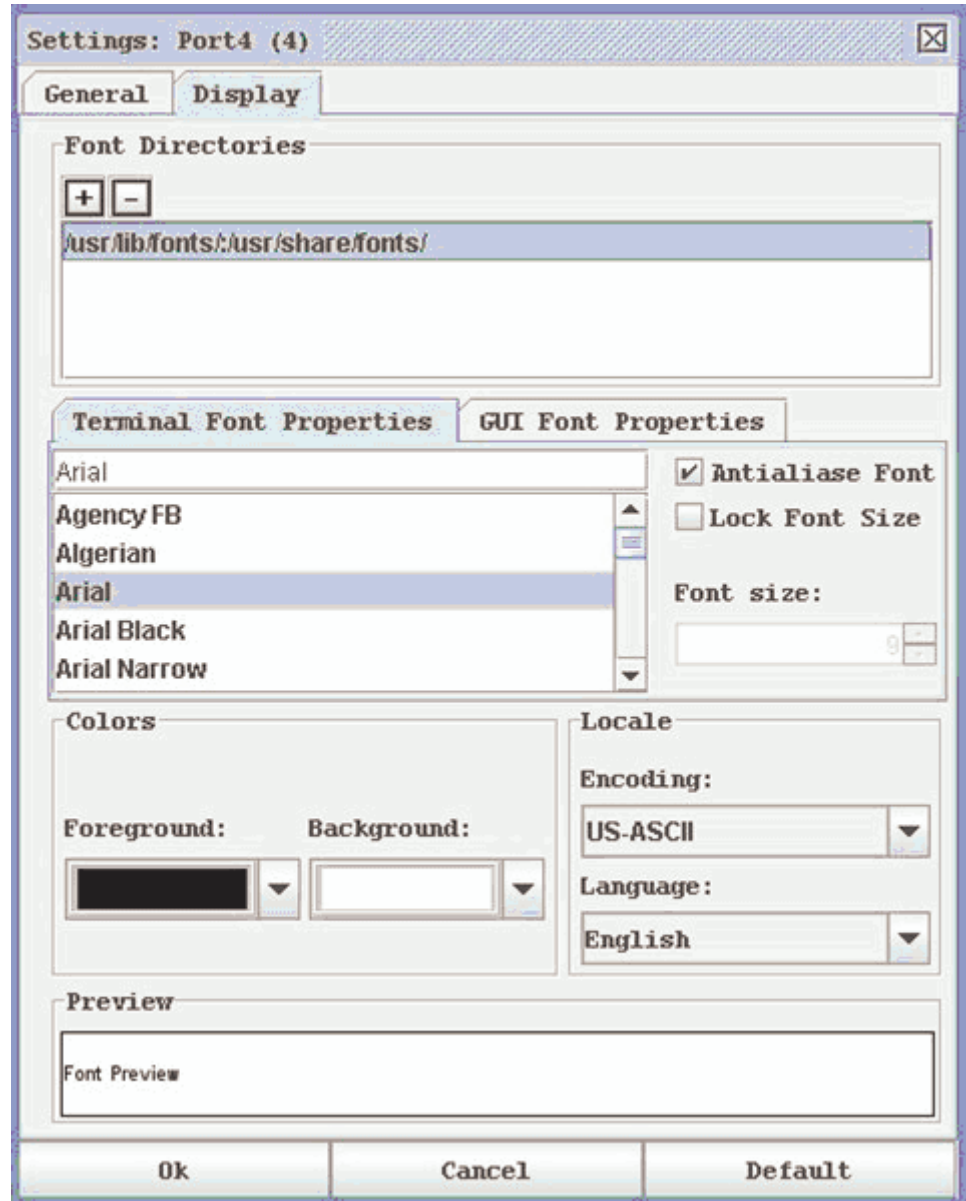
2. Accept the Main Menu Shortcut: default of None or choose one of the following from the Main Menu Shortcut: drop-down menu.
  - F10
  - Alt
3. Accept the Show Confirmation Dialog on Exit default or uncheck it.
4. Accept the Terminal Size: default or choose a size from the Terminal Size: drop-down menu.

## **Raritan Serial Client Interface**

5. Accept the Backspace Sends: default of ASCII DEL or choose Control-H from the Backspace Sends: drop-down menu.
6. Accept the History Buffer Size: default of 200 or use the arrows to change the buffer size.
7. Accept the Cursor type: default of Block Cursor: or select Line Cursor.
8. Click OK.

**Display Settings**

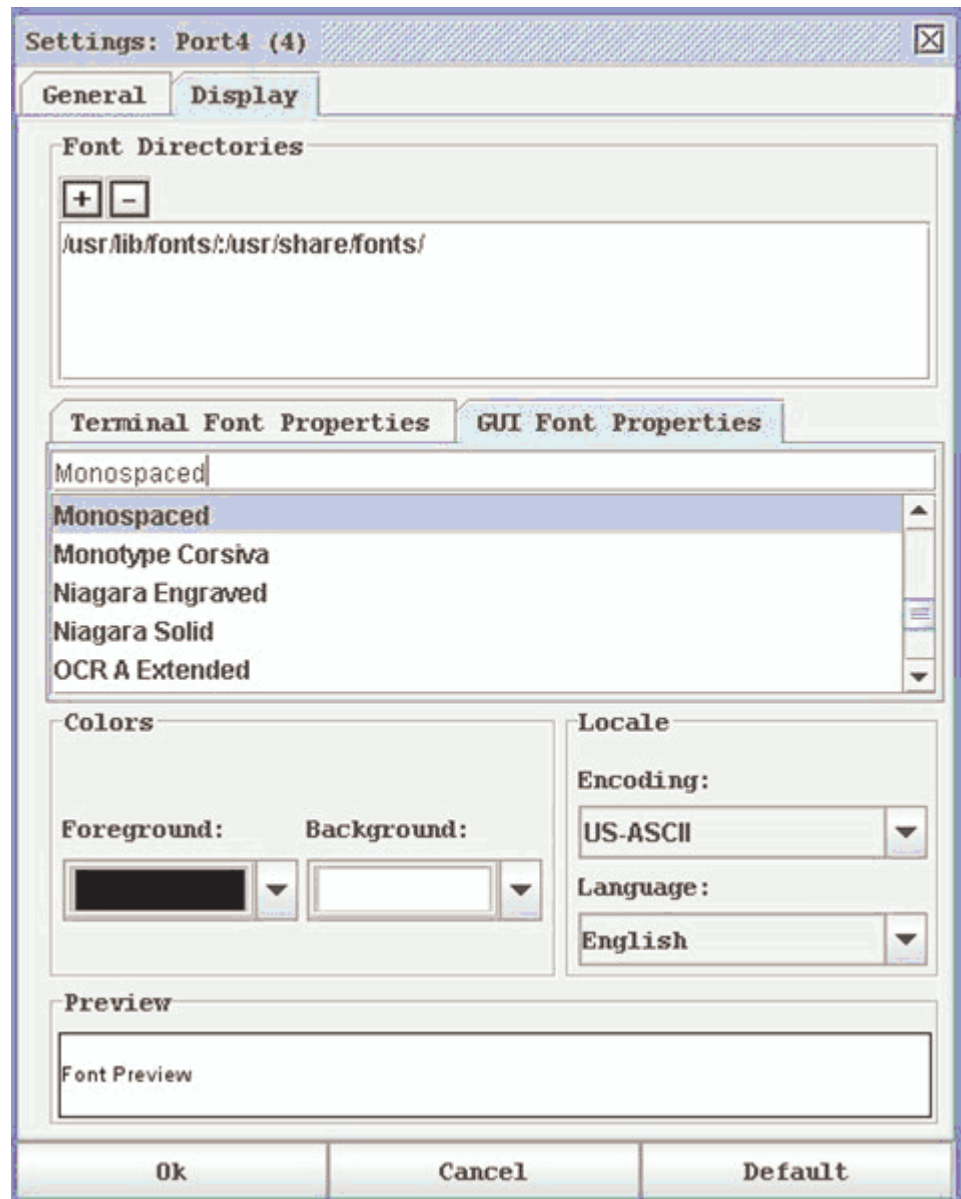
1. Return to the Emulator menu, choose Settings and then click the Display tab.



2. Click Default to accept the Default settings. Then click Ok to close the Display Settings window; however, if you want to change the settings, perform the following steps:
3. Accept the Terminal Font Properties default of Arial or choose a font from the Terminal Font Properties scrolling list.
4. Accept the Antialiase Font default or uncheck it.

## Raritan Serial Client Interface

5. If you want to change the size of the font, check the Lock Font Size box and choose a font size from the Font size: drop-down menu.
6. Click the GUI Font Properties tab and accept the default of Monospaced or choose a font from the GUI Font Properties scrolling list.



---

Note: For Simplified Chinese characters, Raritan Serial Console supports EUC-CN encoding system.

---

7. Choose the following from their drop-down menus:
  - Foreground Color



- Background Color
8. Choose one of the following from the Encoding drop-down menu:
    - US-ASCII
    - ISO-8859-1
    - ISO-8859-15
  9. Choose one of the following from the Language drop-down menu:
    - English
    - Japanese
    - Korean
    - Chinese
  10. Click Ok to close the Display Settings window. If you changed the Language setting, the RSC changes to that language when the Display Settings window is closed.

---

*Note: In case of unrecognized characters or blurry screens that might appear when RSC is launched due to localization support, please try changing the font to Courier New.*

---

### **Get History**

History information can be useful when debugging, troubleshooting, or administering a target device. The Get History feature:

- Allows you to view the recent history of console sessions by displaying the console messages to and from the target device.

When the size limit is reached, the text will wrap, overwriting the oldest data with the newest.

---

*Notes: Verify the memory on your unit from the Maintenance->Configuration menu. History data is displayed only to the user who requested the history.*

---

To view the Session History, click Get History on the Emulator menu.

### **Clear History**

- To clear the history, click Clear History on the Emulator menu.

## Raritan Serial Client Interface

### Get Write Access

Only Administrators and Operators can get write access. The user with Write Access can send commands to the target device. Write Access can be transferred among users working in the Raritan Serial Console via the Get Write Access command.

To enable Write Access, click Get Write Access on the Emulator menu.

- You now have Write Access to the target device.
- When another user assumes Write Access from you,
  - The RSC displays a red block before Write Access in the status bar.
  - A message alerting the user who currently has Write Access appears to tell that user that another user has taken over access to the console.

### Get Write Lock

1. To get write lock, click Get Write Lock on the Emulator menu.
2. If the Get Write Lock is not available, a request rejected message appears:

### Write Unlock

To get Write Unlock, click Write Unlock on the Emulator menu.

### Send Break

Some target systems such as Sun Solaris servers require the transmission of a null character (Break) to generate the **OK** prompt. This is equivalent to issuing a STOP-A from the Sun keyboard.

- Only users with Administrator privileges can send a break.
- Users who are Operator or Observers cannot send a break.

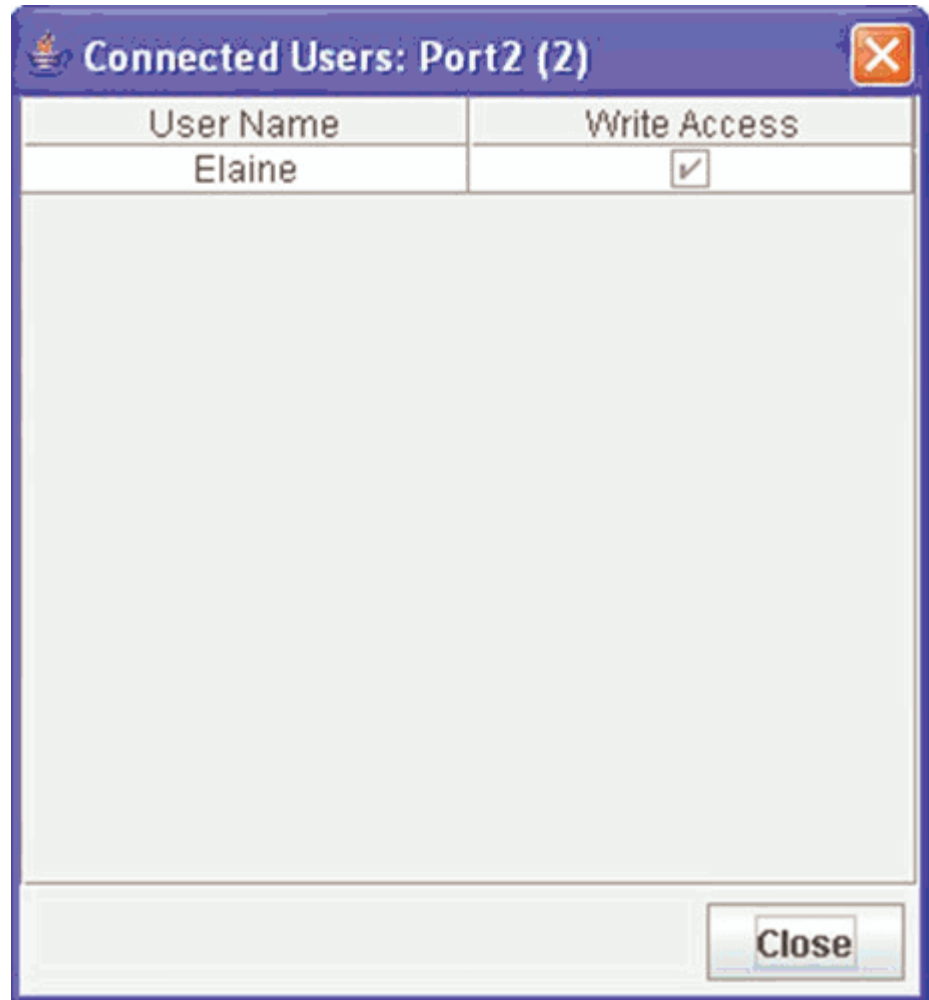
To send an intentional “break” to a Sun Solaris server:

1. Verify that you have Write Access. If not, follow the instructions in the previous section to obtain write access.
2. Click Send Break on the Emulator menu.  
A Send Break Ack (Acknowledgement) pop-up appears.
3. Click OK.

**Connected Users**

The Connected Users command allows you to view a list of other users who are currently connected on the same port.

1. Click Connected Users to view the connected users on the Emulator menu.



2. A check mark appears in the Write Access column after the name of the User who has Write Access to the console.
3. Click Close to close the Connected Users window.

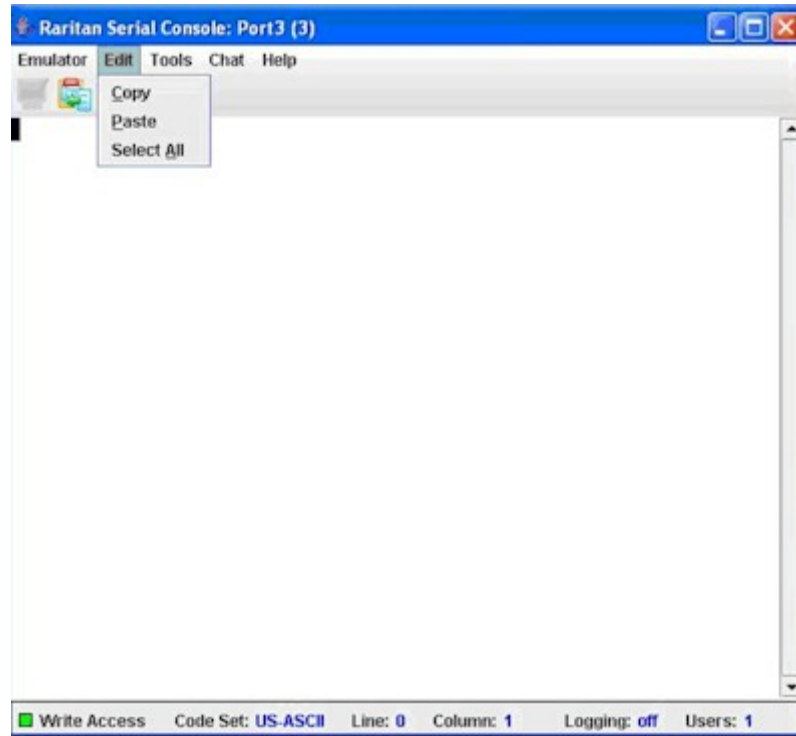
**Exit**

1. Click Exit on the Emulator menu to close the Raritan Serial Console. The Exit Confirmation screen appears.
2. Click Yes.

## Raritan Serial Client Interface

### Edit

Use the Copy, Paste, and Select All text commands to relocate and/or re-use important text.



#### ➤ **Copy and Paste All Text:**

1. Click Select All on the Edit menu.
2. Click Copy on the Edit menu.
3. Position the cursor at the location where you want to paste the text.
4. Click once to make that location active.
5. Click Paste on the Edit menu.

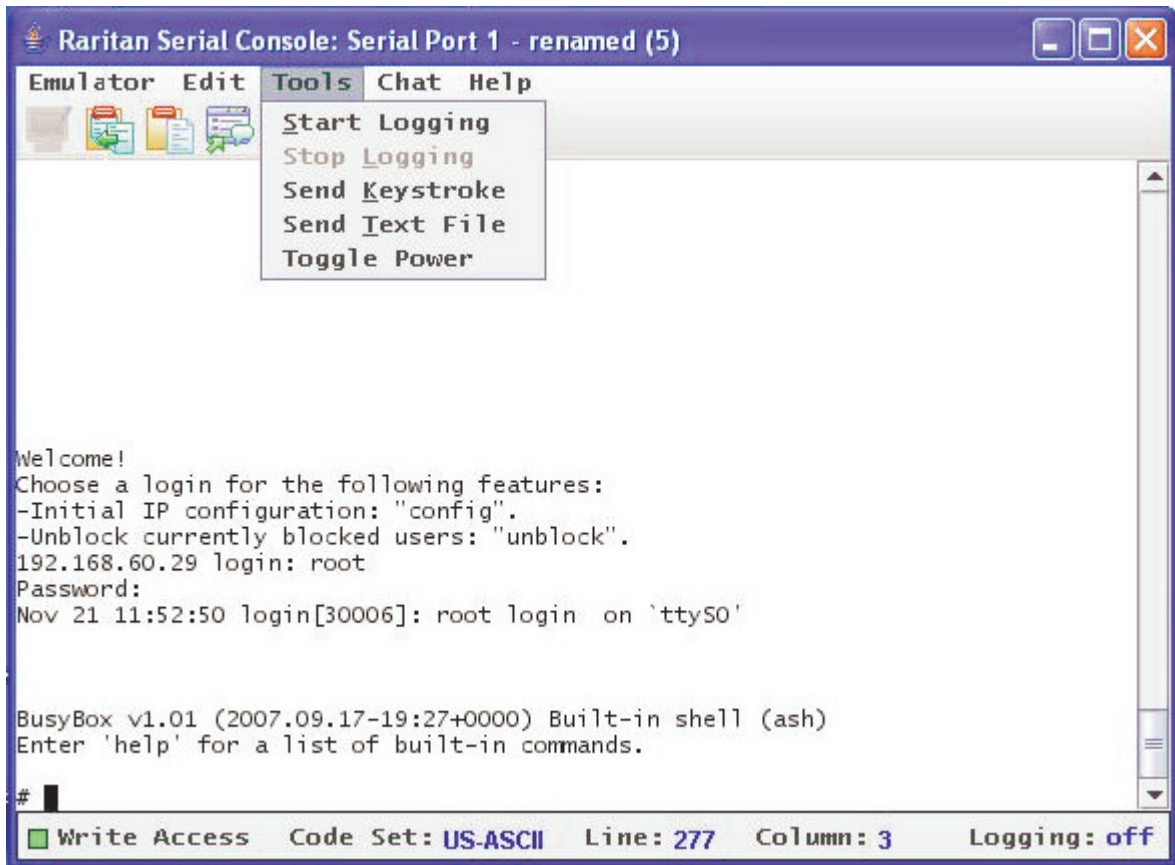
Note: Here are keyboard shortcuts that you can use to highlight, copy, and paste all or partial lines of text:

- Click and drag your mouse over the text you wish to copy.
- Press CTRL and tap the C key to copy.
- Position the cursor where you want to paste the text and click in that location to make it active.
- Press CTRL and tap the V key to paste.

The text copy limit in Raritan Serial Console is 9999 lines.

### Tools

Click on the Tools drop-down menu to display a list of topics.

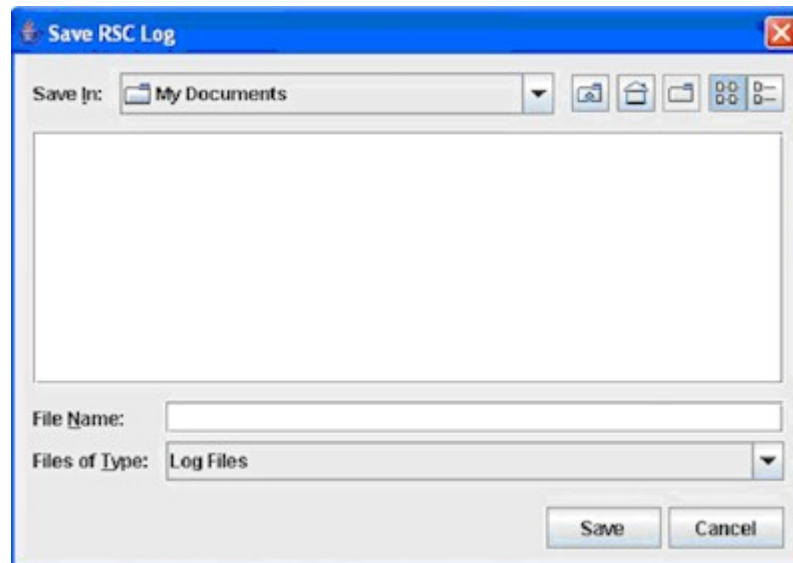


## Raritan Serial Client Interface

### Start Logging

The Start Logging function allows you to collect raw console data from the target device and save it to a file in your computer. When you start the RSC, the Logging indicator on the status bar indicates whether logging is on or off.

1. On the Tools menu, click Start Logging.
2. Choose an existing file or provide a new file name in the Save RSC Log dialog.
  - When an existing file is selected for logging, data gets appended to the contents.
  - Providing a new file name results in new file being created.



3. Click Save after selecting or creating a file.

### Stop Logging

On the Tools menu, click Stop Logging. The logging stops.

### Send Keystroke

1. On the Tools menu, click Send Keystroke.  
A Send Keystroke screen appears:



2. Enter the keystroke combinations that you want and select a Key Code name from the drop-down menu.
3. Send the keystroke combinations.

### Send Text File

1. On the Tools menu, click Send Text File.  
A Send Text File screen appears:
2. Open the directory of the Text file.
3. Click on or enter the File Name of the Text file.
4. Click Open.
  - As soon as you click the Open dialog, it sends whatever file you selected directly to the port.
  - If there is a loopback plug inserted, you see the file displayed.

If there is currently no target connected, then nothing will be visible on the screen.

## Raritan Serial Client Interface

---

### Chat

When using browser access over SSL, an interactive chat feature called Chat provides you and other users on the same port to communicate. You can conduct an online dialog for training or collaborative diagnostic activities. The maximum length of a chat message is 300 characters.

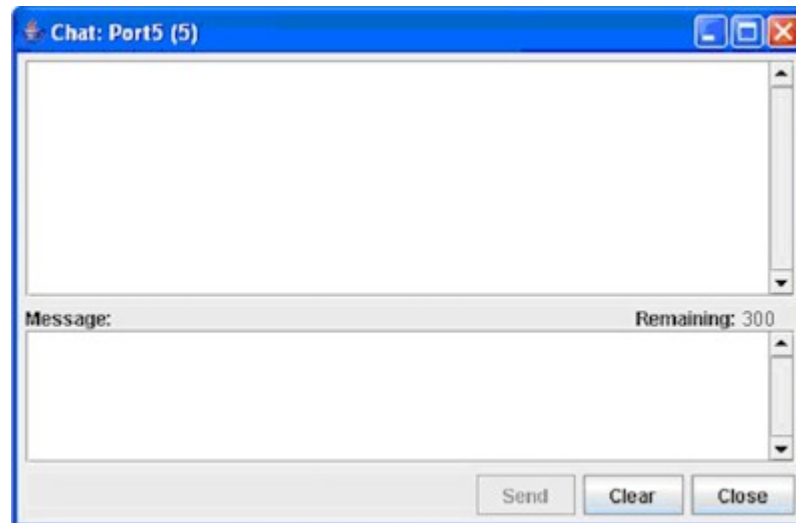
---

*Note: When a chat is initiated, a chat window appears on the monitors of all SSL users logged on to the port. If a user is logged into a port multiple times, chat messages will not be shown to the same user.*

---

#### To use Chat:

1. Click Chat on the Chat menu.



2. Type a message in the Message text field.
3. Click Send or press ENTER to send the message.
4. Click Clear to delete the typed text, or click Close to exit and close the Message window.

---

### Help

Help Topics include on-line assistance for operating the Raritan Serial Console, and release information about Raritan Serial Console.

#### Help Topics

To Access Help Topics:

1. Click Help Topics on the Help menu.



2. Use the navigation bar on the right side of Table of Contents window to scroll to the topic you need or click on the links.
3. Close this window when you are finished.

**About Raritan Serial Console**

The About Raritan Serial Console window displays the copyright and version information (name and revision number) of the console terminal emulation software. When contacting Raritan for technical support or when performing a software upgrade, you may be asked for this information.

➤ **To Access 'About' Information:**

1. Click About Raritan Serial Console on the Help menu.

An About Raritan Serial Console message appears on top of the Raritan Serial Console drop-down menu:



2. Click OK to close the About Raritan Serial Console window.

# Chapter 15 Command Line Interface (CLI)

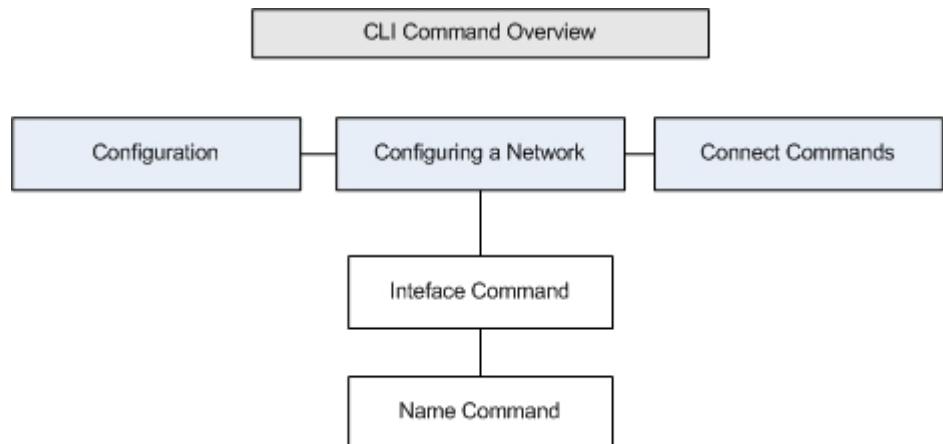
## In This Chapter

Overview .....	234
Accessing the KSX II Using CLI.....	235
SSH Connection to the KSX II.....	236
Telnet Connection to the KSX II.....	236
Local Serial Port Connection to the KSX II.....	237
Login.....	238
Navigation of the CLI.....	240
Initial Configuration.....	242
CLI Prompts.....	243
CLI Commands.....	243
Target Connections and the CLI.....	244
Administering the KSX II Console Server Configuration Commands..	245
Configuring Network.....	245

---

## 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
- 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.

---

*Note: The following figures describe an overview of the CLI commands. See CLI Commands 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, logout, 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) (<http://www.ssh.com>)
- Applet SSH Client - [www.netspace.org/ssh](http://www.netspace.org/ssh)  
(<http://www.netspace.org/ssh>)
- OpenSSH Client - [www.openssh.org](http://www.openssh.org) (<http://www.openssh.org>)

---

### SSH Connection to the KSX II

The SSHv2 Server is configured to run on the KSX II by default. Use any SSH client that supports SSHv2 to connect to it.

---

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

---

SSH should be enabled in Device Settings/Device Services (see *Device Management* (on page 141)). Please refer to *Telnet Connection to the KSX II* (on page 236) for information about enabling Telnet.

---

#### SSH Access from a Windows PC

➤ **To open an SSH session from a Windows PC:**

1. Launch the SSH client software, such as PuTTY.
2. Enter the IP address of the KSX II server 192.168.0.192.
3. Choose SSH, which uses the default configuration port 22.
4. Click the Open button.
5. The following prompt appears:  
login as:

See the Login section for login information.

---

#### SSH Access from a UNIX Workstation

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

```
ssh -l admin 192.168.30.222
```

The following prompt appears:

```
password:
```

See the Login section for login information.

---

### Telnet Connection to the KSX II

Due to the lack of security, username, 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.

#### Browser (GUI)

Enable Telnet access in the Device Settings > Device Services menu.

#### Accessing the KSX II Unit

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

---

### TELNET Access from a Windows PC

➤ **To open a Telnet session from a PC:**

1. Choose Startup > Run.
2. Type `Telnet` in the Open text box.
3. Click OK. The Telnet window opens.
4. At the prompt enter the following command  
Microsoft Telnet> `open <IP address>`  
where <IP address> is the KSX II IP address set up in Assigning an IP Address.
5. Press Enter. The following message appears:  
Connecting To <IP address>...
6. The following prompt appears:  
login as:
7. See the Login section for login information.

---

### 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 there is an RJ 45 interface, 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 a KSX II device as a serial target to another KSX II.

## Login

---

### 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

---

## Login

➤ **To log in, enter the user name *admin* as shown:**

```
login as: admin
```

The password prompt appears. Enter the default password: *raritan*

```
Password:
```

The welcome message displays. You are now logged in as an Administrator.

```

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 >

```

## Navigation of the CLI

```
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 >
```

After reviewing the following *Navigation of the CLI* (on page 240) section, perform the Initial Configuration tasks.

---

## Navigation of the CLI

Before using the CLI, it is important to understand CLI navigation and syntax. Additionally, there are combinations of keystrokes that simplify CLI use.

---

### Completion of Command

The CLI supports the completion of partially entered commands. After entering the first few characters of an entry, hit 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 greater than one possible match is found, the CLI also displays the valid entries.
- The user can enter additional text to make the entry unique and 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.
- A question mark (?) after a command gives help for that command.
- A vertical line ( | ) indicates a choice within an optional or required set of keywords or arguments.

### Shortcuts

- Press the Up-Arrow to display the last entry.
- Use the Backspace key to delete the last character typed.
- Use Ctrl/C to terminate a command or cancel a command if you typed the wrong parameters.
- Use Enter to execute the command.
- Press Tab to complete a command, such as:  
admin > Conf
- The system displays the admin > Config > prompt.

---

## Common Commands for all Command Line Interface Levels

CLI Commands lists the commands that are available at all CLI levels. These commands also help navigate through the CLI.

Command	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

---

*Note: These steps, which use the CLI, are optional since the same configuration can be done via KVM. See **Getting Started** (on page 15) for more information.*

---

KSX II units come from the factory with default factory settings. When you first power up and connect to the unit, 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 units 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, gateway IP address to allow remote access.

---

### Setting Parameters

To set parameters the user must be logged in with administrative privileges. At the top level the user will see the "Username" > prompt, which for initial configuration is "admin" >. If the user has logged in with a different user name, that user name will appear instead of admin. Enter the top command to return to the top menu level.

---

### Setting Network Parameters

Network parameters are configured using the interface command.

```
admin > Config > Network > interface enable true if  
lan1 ip 192.16.151.12 mask 255.255.255 gw  
192.168.51.12
```

When the command is accepted, the unit automatically drops the connection. You must reconnect to the unit using the new IP address and the username admin and password newp/w entered 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 rear panel and the initial configuration tasks will need to be performed again.**

---

The KSX II now has the basic configuration and can be accessed remotely via SSH, GUI or locally using the local serial port. Next, 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; admin is the root portion in the following command:

```
admin > Config > Port >
```

---

## 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.

## Target Connections and the CLI

---

### Security Issues

There are a number of elements to consider when addressing security for console servers:

- Encrypting the data traffic sent between the operator console and the KSX II unit.
- Providing authentication and authorization for users.
- Logging data relevant to the operation for later viewing and auditing purposes. In some cases, this data is required for compliance with governmental or company regulations.
- Security profile

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 unit 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 is displayed. The KSX II unit also provides the ability to share ports among users.

---

### Set Emulation on Target

To set emulation on the target:

- Ensure that the encoding in use on the host matches the encoding configured for the target device. For example, 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. For example, 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 unit is a property associated with the port settings for a particular target device. Ensure that the settings for terminal emulation in the client software, for example, 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 access in the Configuration menu for the KSX II.

---

## **Configuring Network**

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

Command	Description
interface	Configure the KSX II unit network interface.
name	Network name configuration

---

### 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	Query 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.

# Chapter 16 CC Unmanage

## In This Chapter

Overview .....	248
Removing KSX II from CC-SG Management .....	249

---

## Overview

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 is displayed (after entry of a valid username and password):



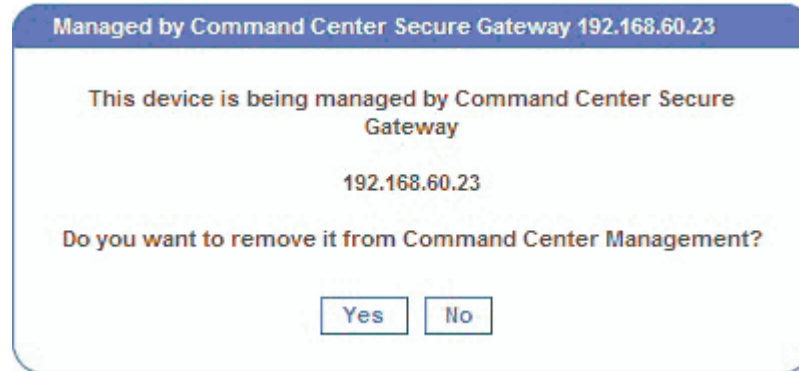


## Removing KSX II from CC-SG Management

Unless the KSX II is released from CC-SG control, you cannot access the device directly. If, however, the KSX II does not receive heartbeat messages from CommandCenter (e.g., CommandCenter is not on the network), you can release the KSX II from CC-SG control in order to access the device. This is accomplished by using the CC Unmanage feature.

*Note: Maintenance permission is required to use this feature.*

When no heartbeat messages are received, the following message is displayed when attempting to access the device directly:



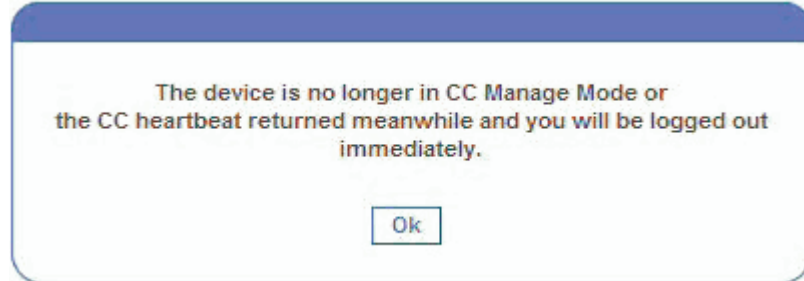
➤ **To remove the device from CC-SG management (to use CC Unmanage):**

1. Click the Yes button. You are prompted to confirm the action:



## Removing KSX II from CC-SG Management

2. Click the Really Unmanage button. A message is displayed confirming that the device is no longer under CC management:



3. Click OK. The KSX II login page opens.

# Chapter 17 Modem Configuration

## In This Chapter

Certified Modems for UNIX, Linux and MPC.....	251
Client Dial-Up Networking Configuration.....	251
Windows NT Dial-Up Networking Configuration.....	251
Windows 2000 Dial-Up Networking Configuration .....	254
Windows XP Dial-Up Networking Configuration .....	258

---

## 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

---

## 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 NT
- Windows 2000
- Windows XP
- Windows Vista

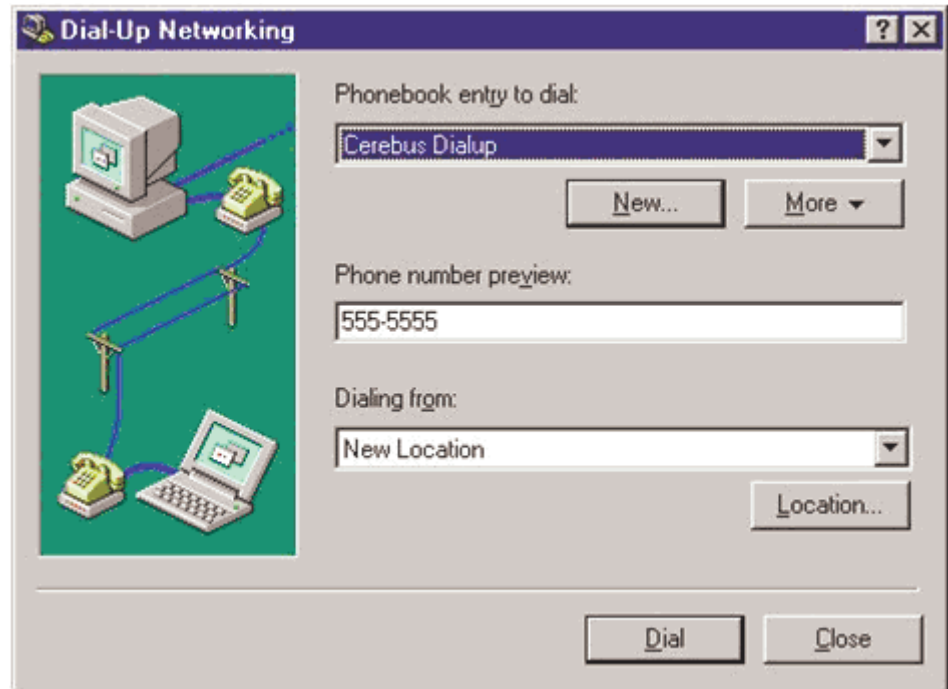
---

## Windows NT Dial-Up Networking Configuration

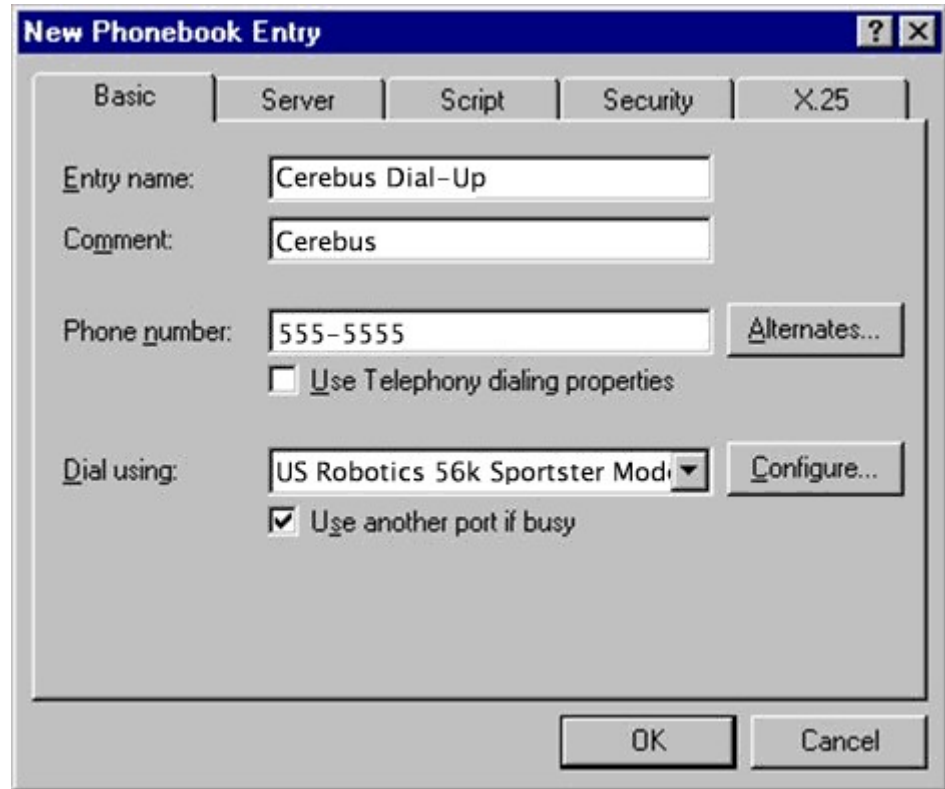
1. Choose Start > Programs > Accessories > Dial-Up Networking.

## Windows NT Dial-Up Networking Configuration

2. Click New.



The New Phonebook Entry window allows you to configure the details of this connection.

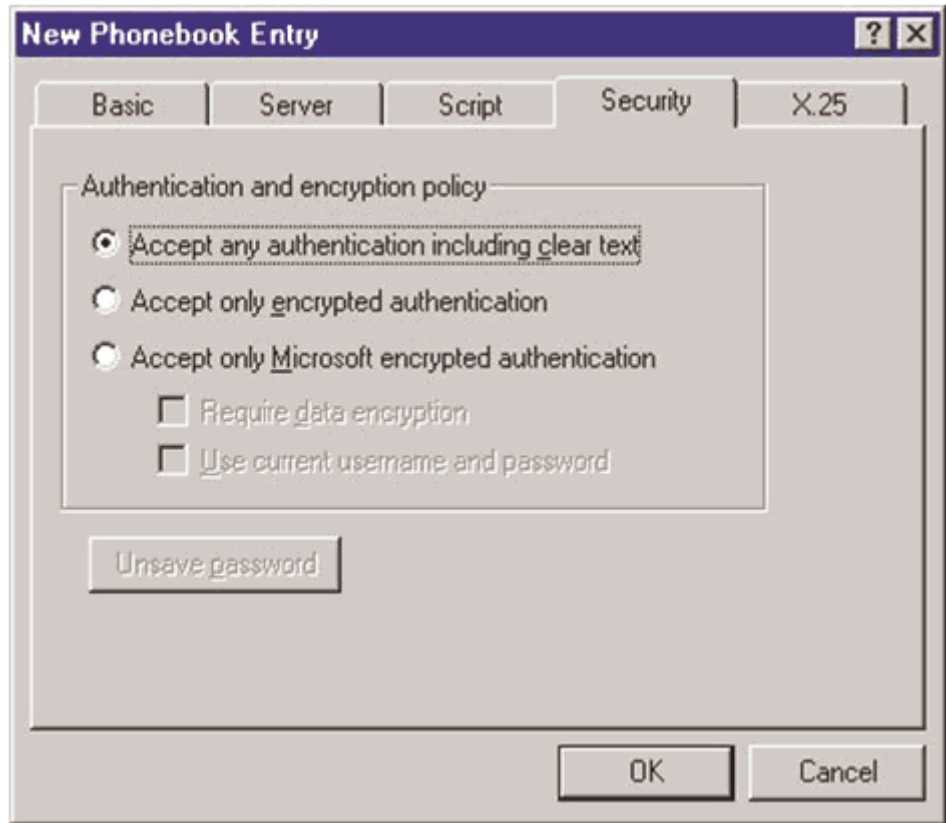


3. Click on the Basic tab and complete the following fields:
  - Entry name: Name of the KSX II connection
  - Phone number: Phone number of the line attached to the KSX II unit
  - Dial using: Modem being used to connect to KSX II; if there is no entry here, there is no modem installed in your workstation
4. Click the Security tab.

The Security section allows you to specify the level of security to use with the modem connection. When connecting to the KSX II unit, security is provided by SSL/ with RC4 encryption, therefore no dialup security is required.
5. Click the Accept any authentication including clear text radio button.

## Windows 2000 Dial-Up Networking Configuration

6. Click OK to return to the main Dial screen.



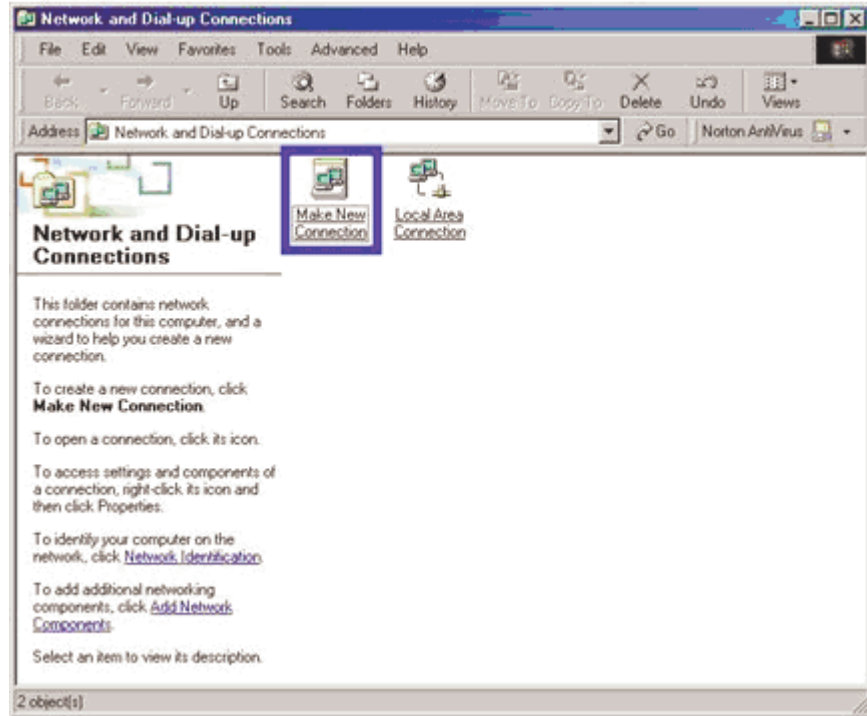
7. Click Dial. See the Windows NT Users Guide if you receive any error message.

---

## Windows 2000 Dial-Up Networking Configuration

1. Choose Start > Programs > Accessories > Communications > Network and Dial-Up Connections.

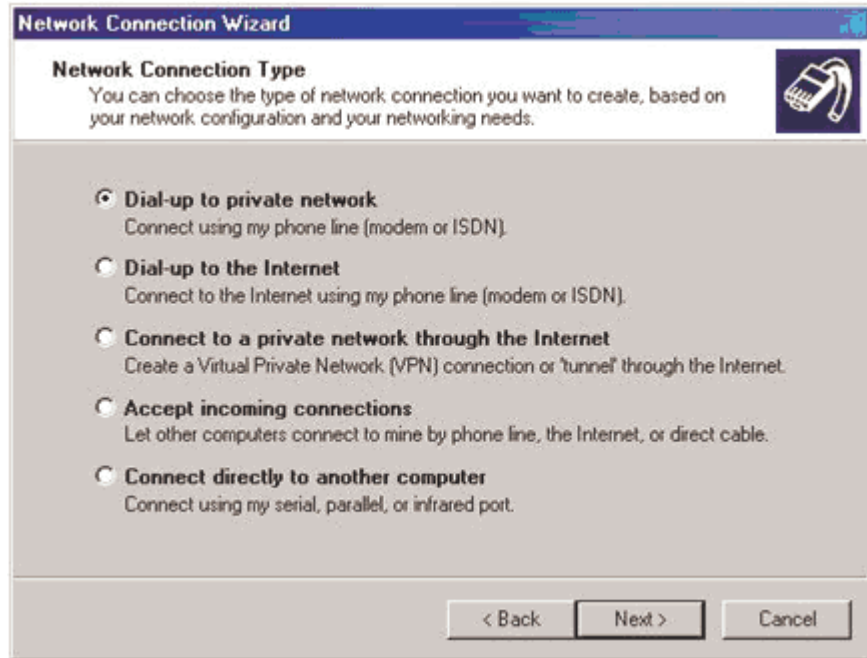
2. Double-click the Make New Connection icon when the Network and Dial-Up Connections window appears.



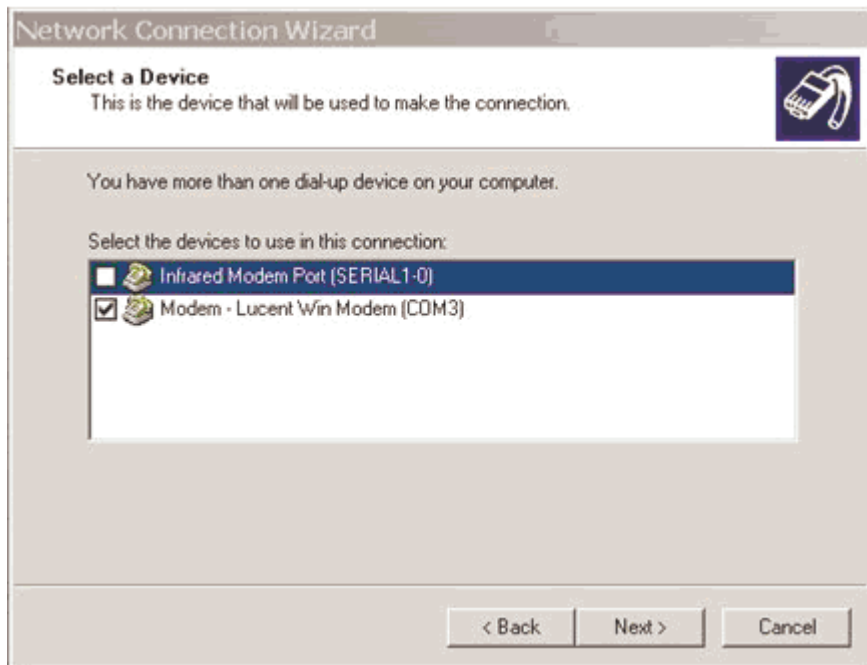
3. Click Next and follow the steps in the Network Connection Wizard window to create custom dialup network profiles.

## Windows 2000 Dial-Up Networking Configuration

- Click the Dial-up to private network radio button and click Next.



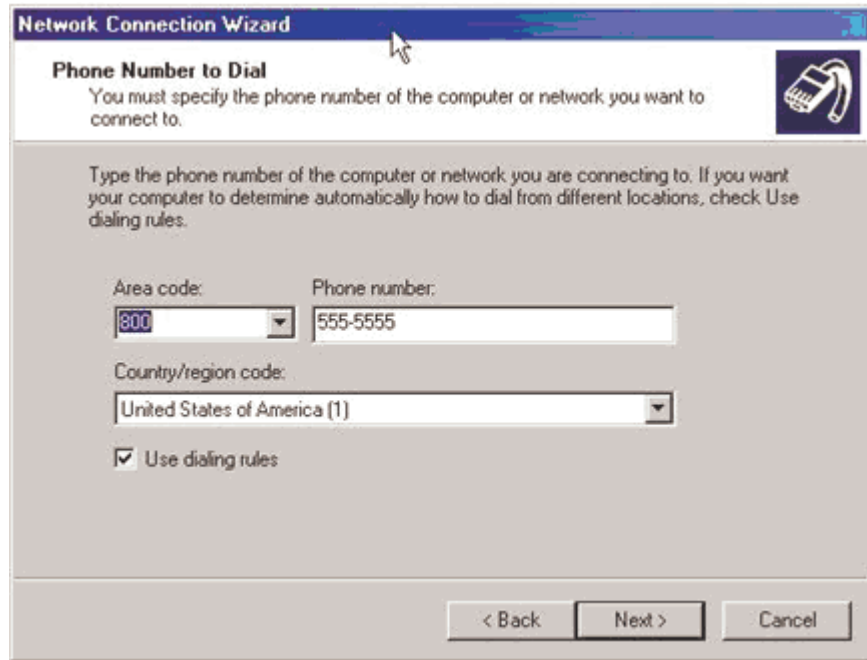
- Select the check box before the modem that you want to use to connect to the KSX II unit and then click Next.



- Type the Area code and Phone number you wish to dial in the appropriate fields.



7. Click the Country/region code drop-down arrow and select the country or region from the list.
8. Click Next.

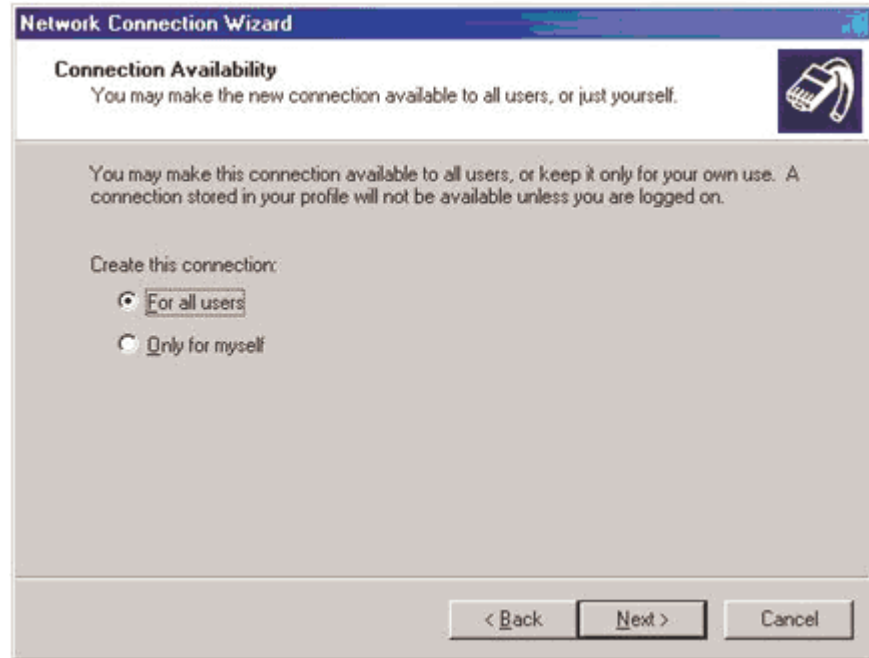


The Connection Availability Screen appears.

9. Click the **Only for myself** radio button in the Connection Availability screen.

## Windows XP Dial-Up Networking Configuration

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 Window appears.

A window indicating that a successful connection has been established will appear.

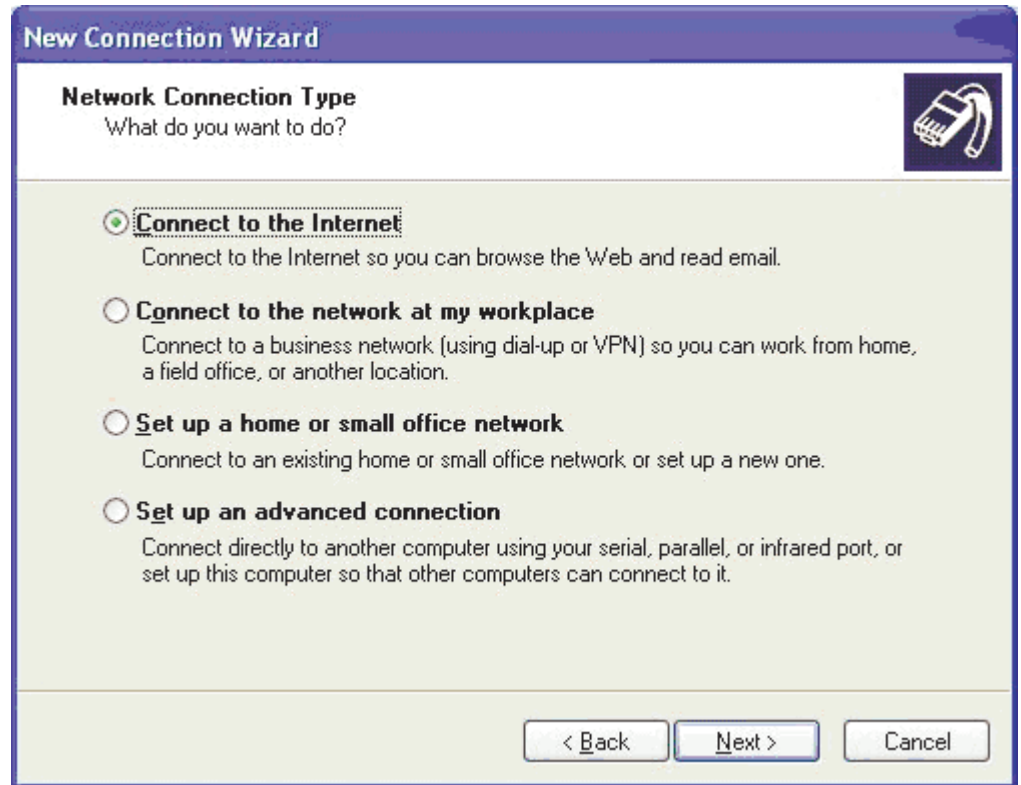
Consult the Windows 2000 Dial-up Networking Help if you receive any error messages.

---

## Windows XP Dial-Up Networking Configuration

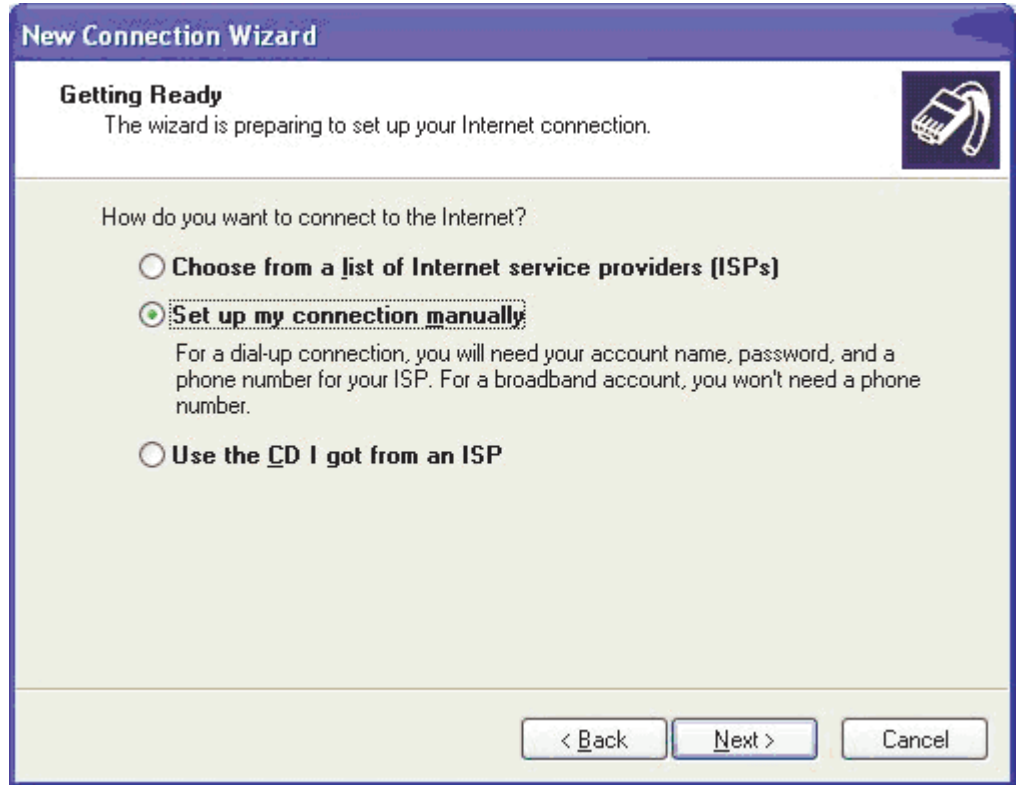
1. Choose Start > Programs > Accessories > Communications > New Connection Wizard.
2. Click Next and follow the steps in the New Connection Wizard to create custom dialup network profiles.

3. Click the Connect to the Internet radio button and click Next.

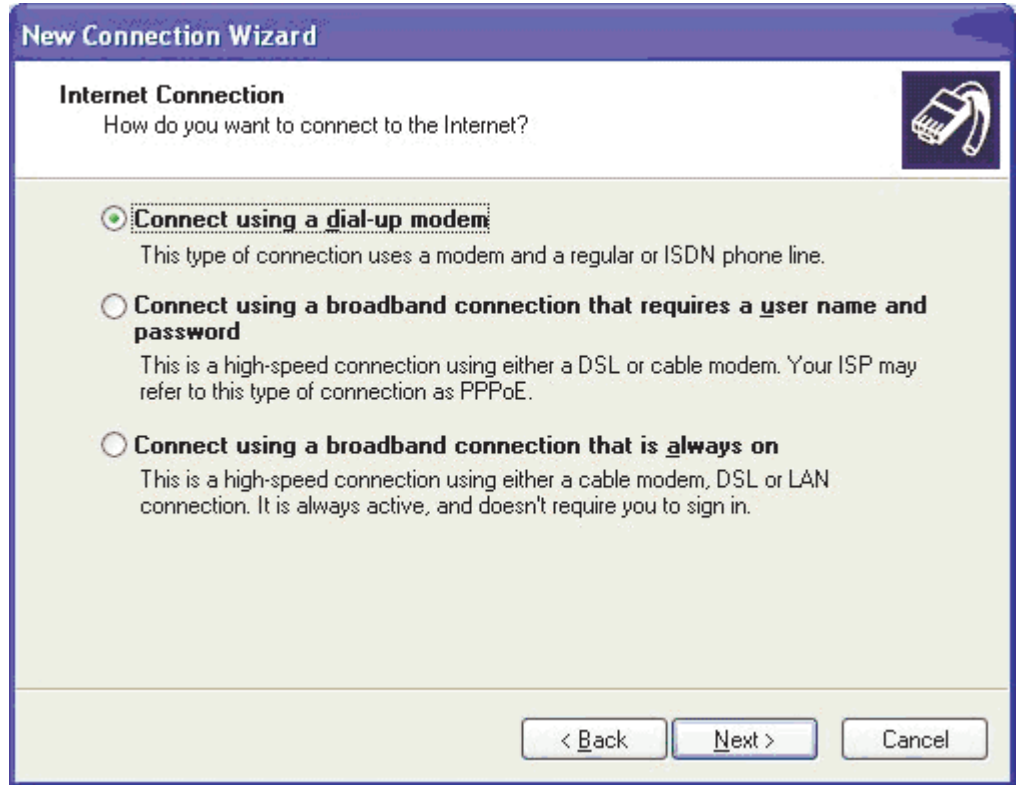


## Windows XP Dial-Up Networking Configuration

4. Click the Set up my connection manually radio button and click Next.



5. Click the radio button before Connect using a dial-up modem and click Next.



## Windows XP Dial-Up Networking Configuration

6. Type a name to identify this particular connection in the ISP Name field and click Next.



**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.

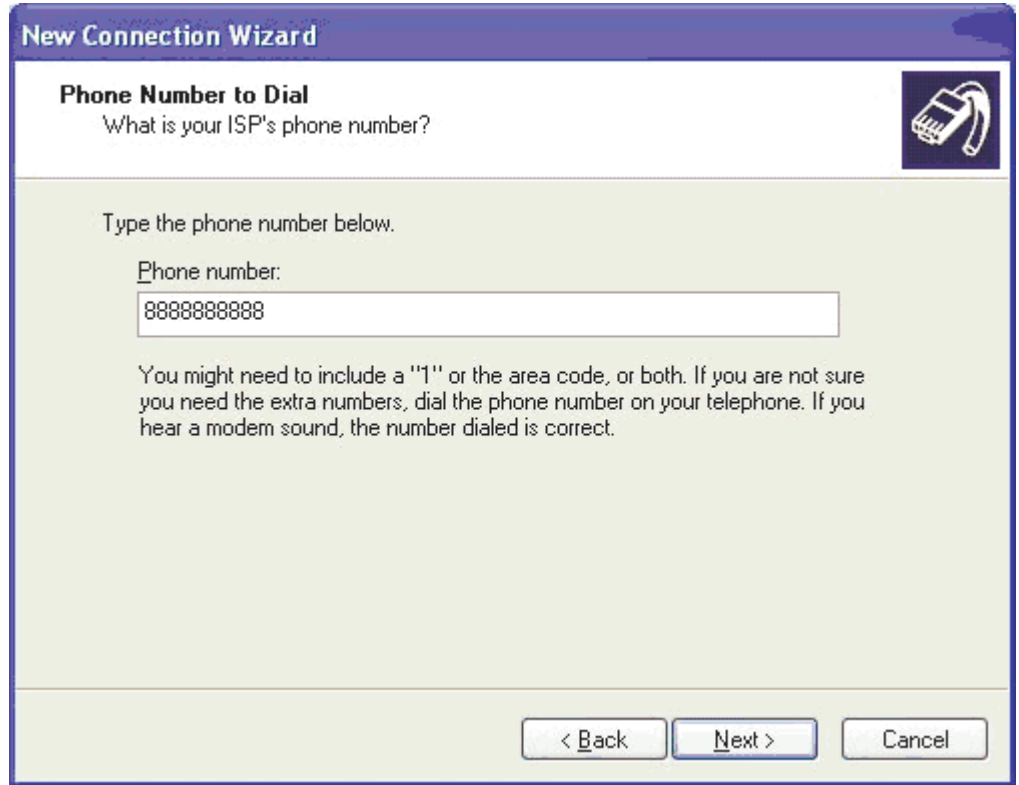
ISP Name

DominionKSX

The name you type here will be the name of the connection you are creating.

< Back   Next >   Cancel


7. Type the phone number of this connection in the Phone number field and click Next.



8. Type your ISP information; type the User name and Password in the appropriate fields, and retype the password to confirm it.

## Windows XP Dial-Up Networking Configuration

- Click the checkbox before the appropriate option below the fields and click Next.



The screenshot shows the 'New Connection Wizard' dialog box with the 'Internet Account Information' step selected. The title bar reads 'New Connection Wizard'. Below the title bar, the section is titled 'Internet Account Information' with a small icon of a modem. The text below the title says: 'You will need an account name and password to sign in to your Internet account.' Below this, there is a paragraph: '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 seven dots, and 'Confirm password:' with seven dots. Below the input fields are two checkboxes: the first is 'Use this account name and password when anyone connects to the Internet from this computer' and the second is 'Make this the default Internet connection'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- Click Finish.
- Click Dial to connect to the remote machine when the Dial Window appears.

A window 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 KSX II units is 33,600 bps, as it is a linux default limitation.*

---



# Appendix A Specifications

## In This Chapter

Environmental Requirements .....	265
Remote Connection.....	268
KVM Properties.....	268
TCP and UDP Ports Used.....	269
Target Server Connection Distance and Video Resolution .....	270
Distances for Serial Devices.....	270
Network Speed Settings .....	271
Connectivity .....	272
KSX II Serial RJ-45 Pinouts .....	273

---

## Environmental Requirements

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)
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

## Environmental Requirements

### Physical Specifications

Part Number	KSX2144	KSX2188
Line Item Description	4 KVM and 4 Serial Port KSX II with multiple user Network Access and Local Port; Virtual Media.	8 KVM and 8 Serial Port KSX II with multiple user Network Access and Local Port; Virtual Media.
Weight	8.65 lbs; 3.9kg	8.65 lbs; 3.9kg
Product Dimensions (WxDxH)	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm
Shipping Weight	14.85 lbs; 6.7 kg	14.85 lbs; 6.7 kg
Shipping Dimensions (WxDxH)	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	22" x 16.6" x 6.5" 559mm x 422mm x 165mm
UPC Code	785813650054	785813650047
Power	100/240 V 50/60 Hz 0.6A 27 Watts	100/240 V 50/60 Hz 0.6A 27 Watts

### Computer Interface Modules (CIMs)

Part Number	D2CIM-VUSB
Line Item Description	KSX II Computer Interface Module [USB Port with Virtual Media]
Product Weight	0.2 lbs
Product Dimensions (WxDxH)	1.3" x 3.0" x 0.6"

<b>Part Number</b>	<b>D2CIM-VUSB</b>
Shipping Weight	0.2 lbs
Shipping Dimensions (WxDxH)	7.2" x 9" x 0.6"
UPC Code	785813332004

<b>Part Number</b>	<b>DCIM-SUN</b>
Line Item Description	KSX II Computer Interface Module [Sun Port, HD15 Video]
Product Weight	0.2 lbs
Product Dimensions (WxDxH)	1.3" x 3.0" x 0.6"
Shipping Weight	0.2 lbs
Shipping Dimensions (WxDxH)	7.2" x 9" x 0.6"
UPC Code	785813338549

---

**Emergency Connectivity**

- 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 for “crash-cart” applications.

See *Connectivity* (on page 272) for a list of necessary KSX II hardware (adapters and/or cables) for connecting the KSX II to common Vendor/Model combinations.

---

**Electrical Specifications**

<b>Parameter</b>	<b>Value</b>
Input	
Nominal Frequencies	50/60 Hz

## Remote Connection

Parameter		Value
	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

---

## Remote Connection

Network: 10BASE-T, 100BASE-T, and 1000BASE-T (Gigabit)  
Ethernet

Protocols: TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS,  
LDAP/LDAPS

---

## KVM Properties

- Keyboard: PS/2 or USB
- Mouse: PS/2 or USB
- Video: VGA

---

## Ports Used

- HTTP, Port 80 - All requests received by KSX II via HTTP (port 80) are automatically forwarded to HTTPS for complete security. KSX II responds to Port 80 for user convenience, relieving users from having to explicitly type “https://” in the URL field to access KSX II, but while still preserving complete security.
- HTTPS, Port 443 - This port is used for the actual KVM-over-IP communication from the KSX II device to the KVM client on the user's desktop. It cannot be changed..
- KSX II (Raritan KVM-over-IP) Protocol, Configurable Port 5000 - This port is used to discover other KX devices and for communication between Raritan devices and systems, including CC-SG and MPC. By default, this is set to Port 5000, but you may configure it to use any TCP port of your choice (except 80 and 443). For details on how to configure this setting, refer to Network Settings.
- SNTP (Time Server) on Configurable UDP Port 123 (optional) - KSX II offers the optional capability to synchronize its internal clock to a central time server. 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.
- LDAP/LDAPS on Configurable Ports 389 and 636 (optional) - If KSX II is configured to remotely authenticate user logins via the LDAP/LDAPS protocol, ports 389 and 636 will be used, but the system can also be configured to use any port of your designation.
- RADIUS on Configurable Port 1812 (optional) - If KSX II is configured to remotely authenticate user logins via the RADIUS protocol, either port 1812 or 1813 will be used, but the system can also be configured to use any port of your designation.
- RADIUS Accounting on Configurable Port 1813 - If 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.
- SYSLOG on Configurable UDP Port 514 - If 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.
- SNMP Default UDP Ports (optional) - Port 161 is used for inbound/outbound read/write SNMP access and port 162 is used for outbound traffic for SNMP traps.

## Target Server Connection Distance and Video Resolution

- 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.

---

## Target Server Connection Distance and Video Resolution

The maximum supported distance is a function of many factors including the type/quality of Cat 5 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
1600x1200	60	50 ft (15 m)
1280x1024	60	100 ft (30 m)
1024x768	60	150 ft (45 m)

*Due to the multiplicity of server manufacturers and types, OS versions, video drivers, etc. and the subjective nature of video quality, Raritan cannot guarantee performance across all distances in all environments.*

Refer to the Supported Video Resolutions for the video resolutions supported by KSX II.

---

## Distances for Serial Devices

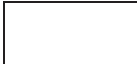
Following are the standard distances for serial devices:

Baud Rate-Feet
2400 - 400ft
4800 - 200ft
9600 - 100ft
19200 - 50ft
38400 - 25ft
57600 - 16ft
115200 - 8ft

**Network Speed Settings**

Dominion KSX II Network Speed Setting							
Network Switch Port Setting		Auto	1000/Full	100/Full	100/Half	10/Full	10/Half
	Network Switch Port Setting	Auto	Highest Available Speed	1000/Full	KSX II: 100/Full Switch: 100/Half	100/Half	KSX II: 10/Full Switch: 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

## Connectivity



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 both the KSX II and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.*

---

## 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	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 CAT 5 cable
Silicon Graphics	Origin		



<b>Vendor</b>	<b>Device</b>	<b>Console Connector</b>	<b>Serial Connection</b>
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 following link to obtain a list of commonly used cables and adapters <http://www.raritan.com/support>

---

### **KSX II Serial RJ-45 Pinouts**

To provide maximum port density and to enable simple UTP (Category 5) cabling, 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.

<b>RJ-45 PIN</b>	<b>SIGNAL</b>
1	RTS
2	DTR
3	TxD
4	GND
5	DCD
6	RxD
7	DSR
8	CTS

Go to the following link to find the latest information about the KSX II serial pinouts (RJ-45).

<http://www.raritan.com/support>

---

**DB9F Nulling Serial Adapter Pinouts**

<b>RJ-45 (Female)</b>	<b>DB9 (Female)</b>
1	8
2	1, 6
3	2
4	SHELL
5	5
6	3
7	4
8	7

---

**DB9M Nulling Serial Adapter Pinouts**

<b>RJ-45 (Female)</b>	<b>DB9 (Male)</b>
1	8
2	1, 6
3	2
4	SHELL
5	5
6	3
7	4
8	7

---

**DB25F Nulling Serial Adapter Pinouts**

<b>RJ-45 (Female)</b>	<b>DB25 (Female)</b>
1	5
2	6, 8

## Appendix A: Specifications

<b>RJ-45 (Female)</b>	<b>DB25 (Female)</b>
3	3
4	1
5	7
6	2
7	20
8	4

---

### DB25M Nulling Serial Adapter Pinouts

<b>RJ-45 (Female)</b>	<b>DB25 (Male)</b>
1	5
2	6, 8
3	3
4	1
5	7
6	2
7	20
8	4

# Appendix B Updating the LDAP/LDAPS Schema

---

*Note: The procedures in this chapter should be attempted only by experienced users.*

---

## In This Chapter

Returning User Group Information.....	276
Setting the Registry to Permit Write Operations to the Schema .....	277
Creating a New Attribute.....	278
Adding Attributes to the Class .....	279
Updating the Schema Cache .....	280
Editing rciusergroup Attributes for User Members .....	281

---

## Returning User Group Information

Use the information in this chapter to return User Group information (and assist with authorization) once authentication is successful.

---

### From LDAP

When an LDAP/LDAPS authentication is successful, 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:

rciusergroup                      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 Server requires updating the LDAP/LDAPS schema. Refer to your Microsoft documentation for more detail.

1. Install the schema plug-in for Active Directory - refer to Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

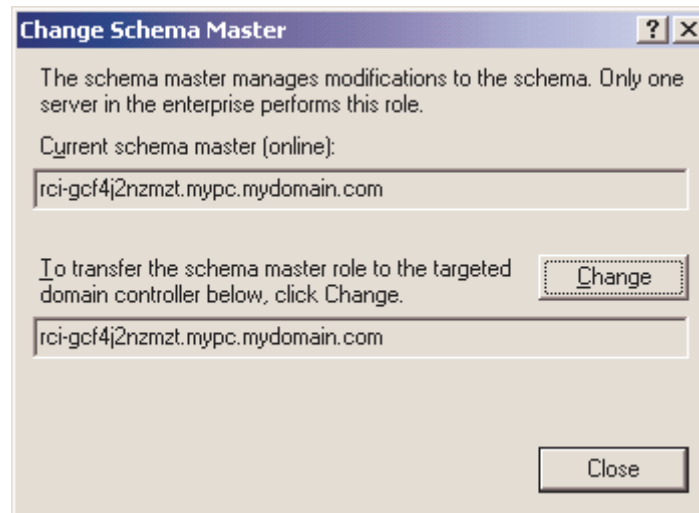
---

## 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 opens:



2. (Optional) Select the checkbox before The Schema can be modified on this Domain Controller.
3. Click OK.

---

### Creating a New Attribute

- **To create new attributes for the *rciusergroup* class:**
1. Click the + symbol before Active Directory Schema in the left pane of the window.
  2. Right-click Attributes in the left pane.
  3. Click New, and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute window opens.

**Create New Attribute**

Create a New Attribute Object

Identification

Common Name: rciusergroup

LDAP Display Name: rciusergroup

Unique X500 Object ID: 1.3.6.1.4.1.13742.50

Description: Raritan's LDAP attribute

Syntax and Range

Syntax: Case Insensitive String

Minimum: 1

Maximum: 24

Multi-Valued

OK Cancel

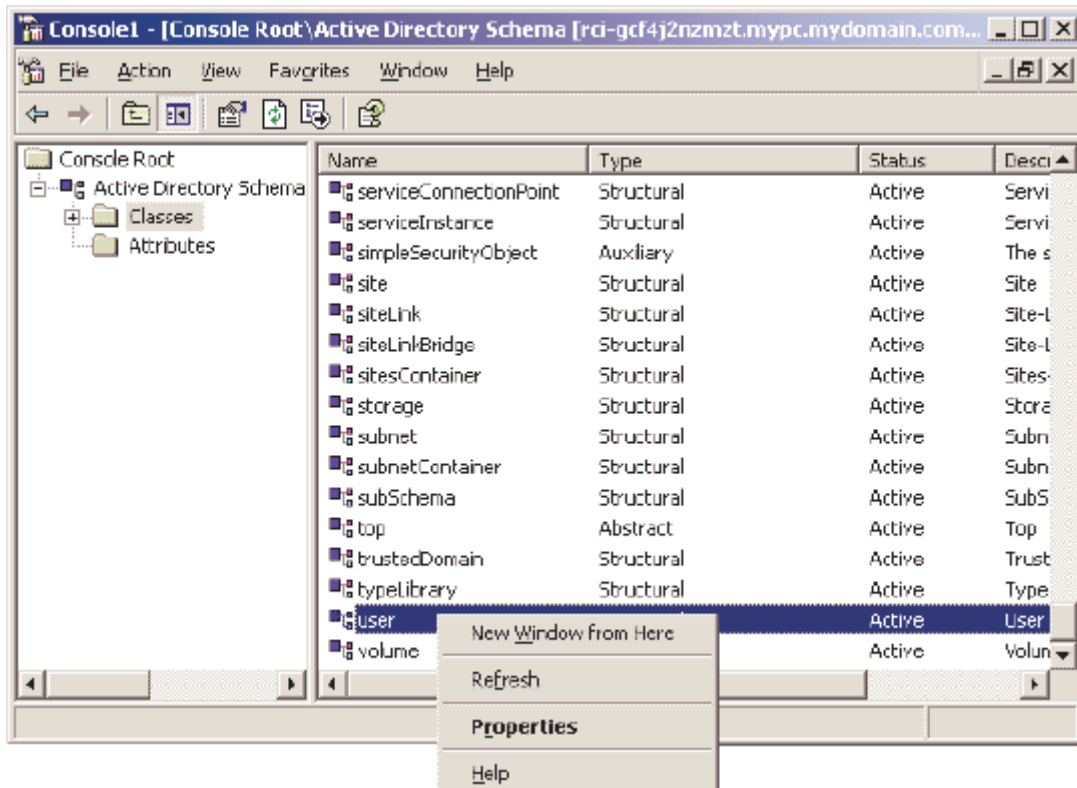
4. Type rciusergroup in the Common Name field.
5. Type rciusergroup in the LDAP Display Name field.
6. Type 1.3.6.1.4.1.13742.50 in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
9. Type 1 in the Minimum field.
10. Type 24 in the Maximum field.

11. Click OK to create the new attribute.

## Adding Attributes to the Class

➤ **To add attributes to the class:**

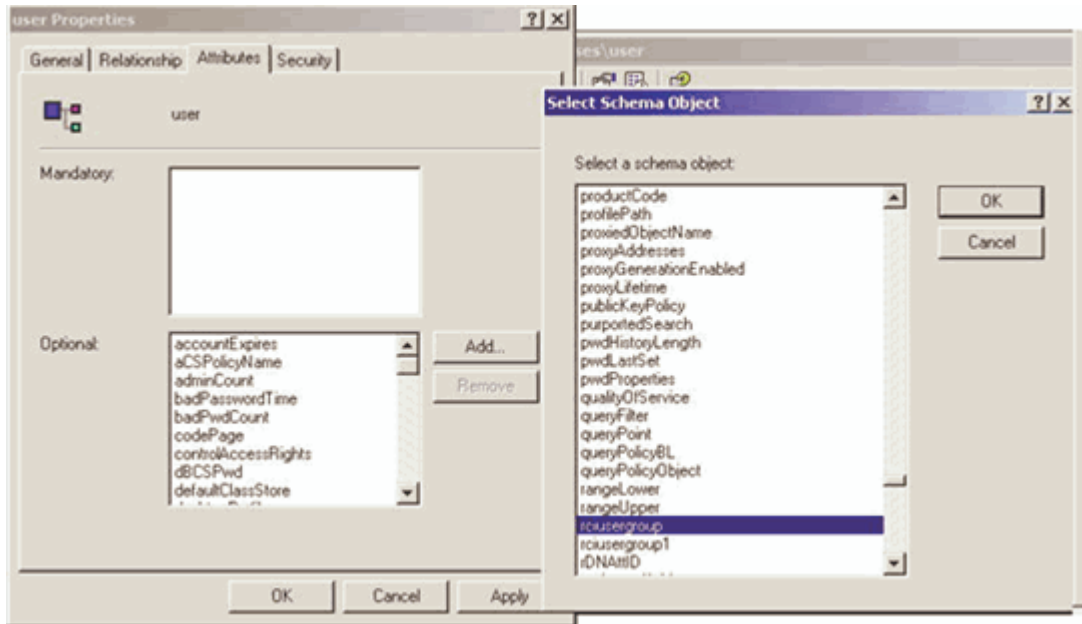
1. Click Classes in the left pane of the window.
2. Scroll to the user class in the right pane, and right-click on it.



3. Choose Properties from the menu. The user Properties window appears.

## Updating the Schema Cache

4. Click on the Attributes tab to open it.



5. Click Add.
6. Choose rcusergroup 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 from the shortcut menu.
  2. Minimize the Active Directory Schema MMC (Microsoft Management Console) console.

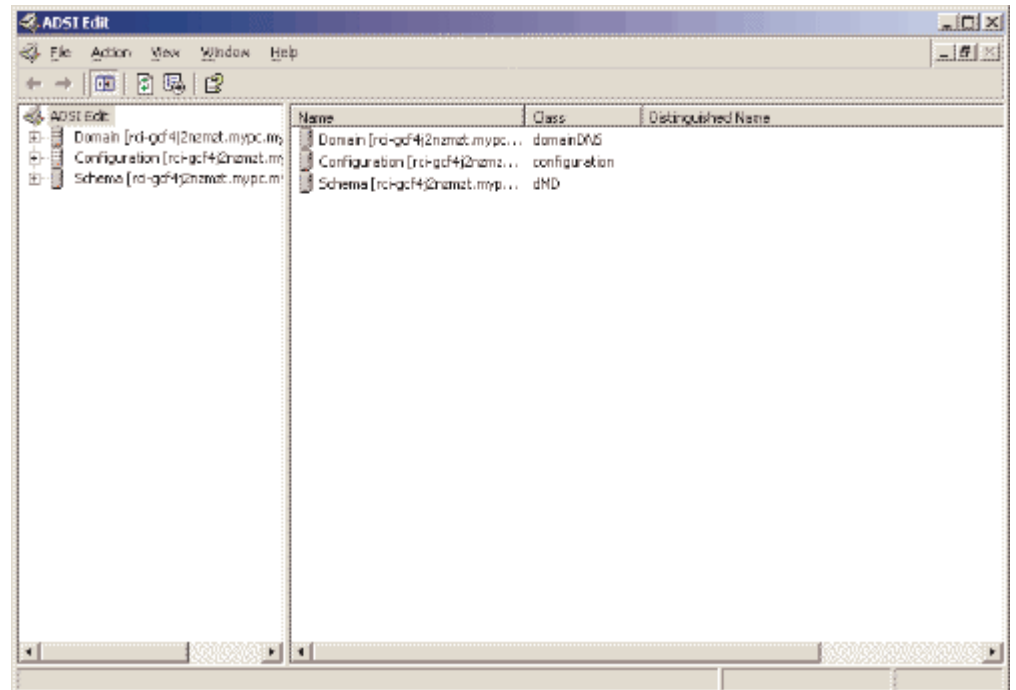


## Editing rcusergroup Attributes for User Members

To run Active Directory script on Windows 2003 server, please 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 rcusergroup:**

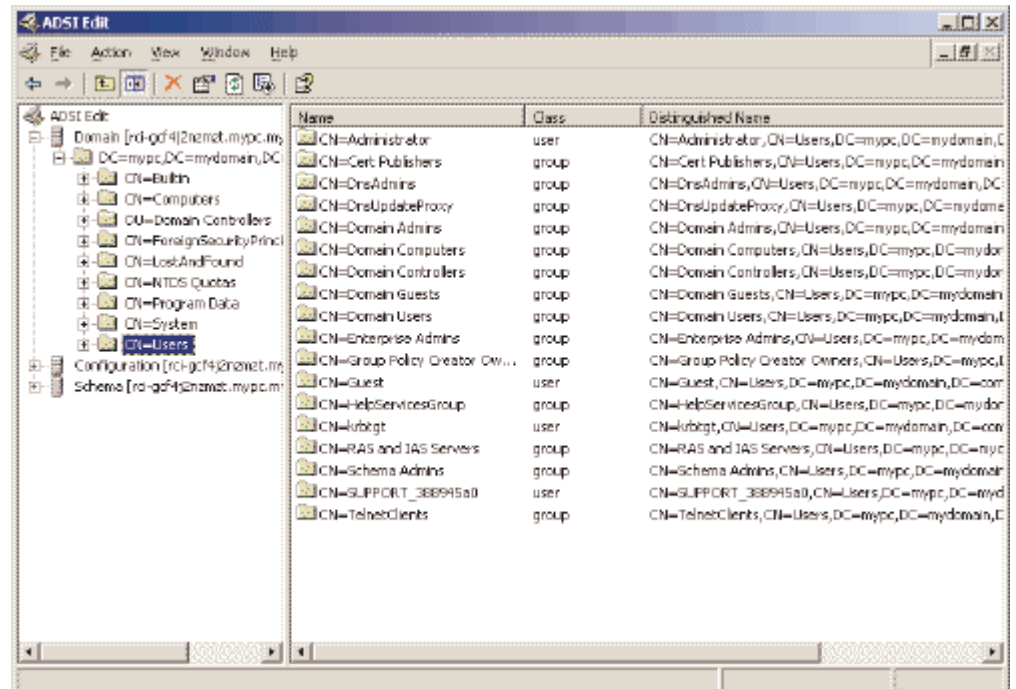
1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.
3. Go to the directory where the support tools were installed.
4. Run adsiedit.msc. The ADSI Edit window opens.



5. Open the Domain.

## Editing rclusergroup Attributes for User Members

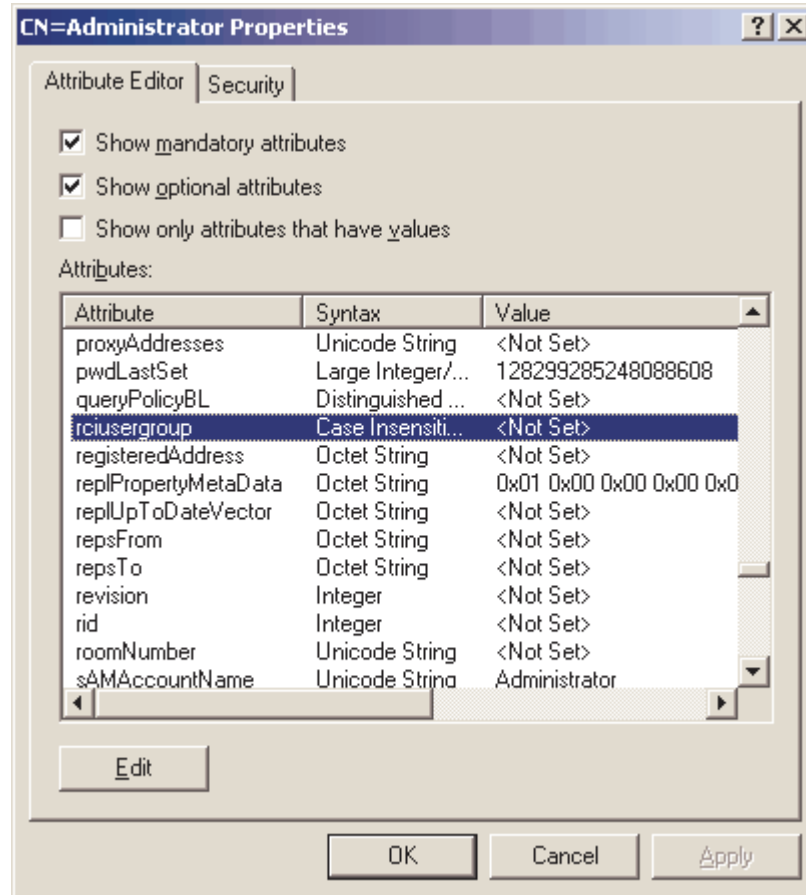
6. In the left pane of the window, select the CN=Users folder.



7. Locate the user name whose properties you want to adjust in the right pane. Right-click on the user name and select Properties.
8. Click on the Attribute Editor tab if it is not already open.

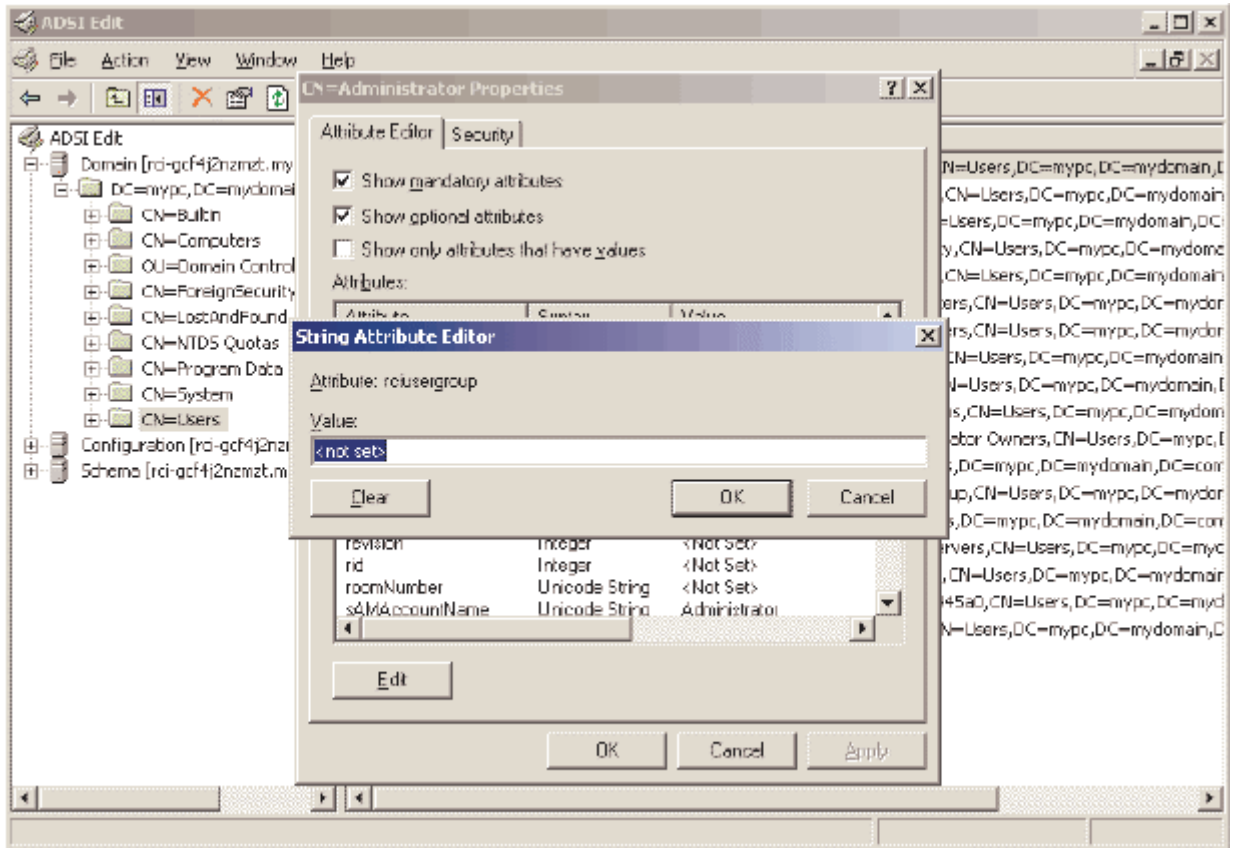
## Appendix B: Updating the LDAP/LDAPS Schema

9. Choose rciusergroup from the Attributes list.

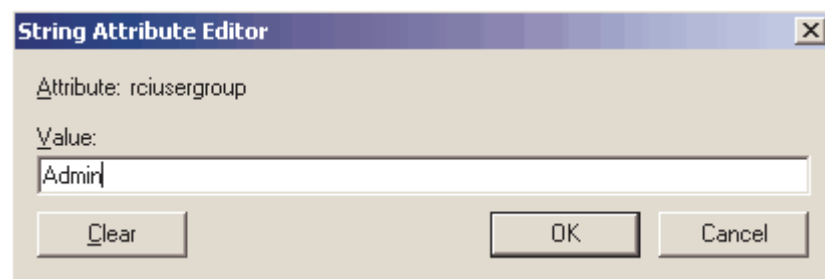


## Editing rclusergroup Attributes for User Members

10. Click Edit. The String Attribute Editor dialog opens:



11. Type the user group (created in Dominion KSX II) in the Edit Attribute field.



12. Click OK.

# Appendix C Informational Notes

In This Chapter

Overview

*Non-US Keyboards* (on page 287)

*Macintosh Keyboard* (on page 290)

Mouse Pointer Synchronization (Fedora)

Resolving Fedora Core Focus

SUSE/VESA Video Modes

CIMs

Virtual Media

CC-SG

## In This Chapter

Overview .....	285
AES_256 Support for Java Clients.....	286
Non-US Keyboards.....	287
Macintosh Keyboard.....	290
Mouse Pointer Synchronization (Fedora).....	290
Resolving Fedora Core Focus.....	291
SUSE/VESA Video Modes.....	291
CIMs.....	292
Virtual Media .....	292
CC-SG .....	293

---

## Overview

This chapter includes important notes on KSX II usage. Future updates will be documented and available online through the Help - User Guide link in the KSX II Remote Console interface.

---

## AES\_256 Support for Java Clients

Application	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	
MPC Applet	Requires installation of Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files +	Browser	Supported
		FireFox 2.0.0.7	Yes
		Mozilla 1.7.13	Yes
		IE 6*	No
HTML access client	Requires installation of Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files +	Browser	Supported
		FireFox 2.0.0.7	Yes
		Mozilla 1.7.13	Yes
		IE 6 *	No
		IE 7	Yes

+ Jurisdiction files for various JRE's are available in the Other Downloads on the Java Sun site.

JRE	Link
JRE1.4.2	<a href="http://java.sun.com/j2se/1.4.2/download.html">http://java.sun.com/j2se/1.4.2/download.html</a> ( <a href="http://java.sun.com/j2se/1.4.2/docs/guide/plugin/developer_guide/control_panel.html">http://java.sun.com/j2se/1.4.2/docs/guide/plugin/developer_guide/control_panel.html</a> )
JRE1.5	<a href="http://java.sun.com/javase/downloads/index_jdk5.jsp">http://java.sun.com/javase/downloads/index_jdk5.jsp</a>
JRE1.6	<a href="http://java.sun.com/javase/downloads/index.jsp">http://java.sun.com/javase/downloads/index.jsp</a>

\* In addition, IE6 does not support AES 128.

---

## **Non-US Keyboards**

---

### **French Keyboard**

#### **Caret Symbol (Linux Clients only)**

The Virtual KVM Client 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.

## Non-US Keyboards

---

*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 Clients only)**

From the Virtual KVM Client and the Multi-Platform Client, 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 and the Multi-Platform Client, the numeric keypad symbols display as follows when using a French keyboard:

<b>Numeric Keypad Symbol</b>	<b>Displays As</b>
/	;
.	;

### **Tilde Symbol**

From the Virtual KVM Client and the Multi-Platform Client, 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



---

### 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 1.4.2 or 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), will only generate 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.

---

### Keyboard Language Preference (Fedora Linux Clients)

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 and the Multi-Platform Client (MPC).

➤ **To set the keyboard language:**

1. From the toolbar, select System > Preferences > Keyboard.
2. Open the Layouts tab.
3. Add or select the appropriate language.
4. Click Close.

---

*Note: Other methods will not necessarily yield correct results.*

---

---

### Macintosh Keyboard

When a Macintosh 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 and the Multi-Platform Client (MPC) are unable to process these keys from a Mac client's keyboard.

---

### Mouse Pointer Synchronization (Fedora)

When connected in dual mouse mode to a target server running Fedora 7, the target and local mouse pointers may lose synchronization after some time.

➤ **To re-synchronize the mouse cursors:**

Use the Synchronize Mouse option from the Virtual KVM Client.

The following table summarizes the KSX II mouse modes, and whether or not these modes remain synchronized when accessing KVM target servers running Fedora:

Mouse Mode	Fedora Core 5	Fedora Core 6
Absolute Mouse Synchronization	No	No
Intelligent Mouse Mode	No	Yes
Standard Mouse Mode	Yes	No

---

## Resolving Fedora Core Focus

Using the Multi-Platform Client (MPC), occasionally there is an inability to log into a KSX II device or to access KVM target servers (Windows, SUSE, etc.). 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 plugin.*

---

---

## 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). 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 will be used and will correspond exactly with the VESA video mode timing, resulting in the proper video display on the KSX II.

---

## CIMs

---

### 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.

---

## Virtual Media

---

### 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.*

---

---

### 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.

---

## CC-SG

---

### **Virtual KVM Client Version not Known from CC-SG Proxy Mode**

When the Virtual KVM Client is launched from CommandCenter Secure Gateway (CC-SG) in proxy mode, the Virtual KVM Client version is unknown. In the About Raritan Virtual KVM Client dialog, the version is displayed as “Version Unknown”.

---

### **Proxy Mode and MPC**

If you are using KSX II in a CC-SG configuration, do not use the CC-SG proxy mode if you are planning to use the Multi-Platform Client (MPC) or the Raritan Serial Client (RSC).

# Appendix D FAQs

## In This Chapter

General Questions.....	294
Serial Access.....	296
Remote Access.....	304
Universal Virtual Media.....	306
Ethernet and IP Networking.....	306
Servers.....	310
Installation.....	310
Local Port.....	312
Power Control.....	314
Scalability.....	315
Security.....	316
Manageability.....	317
Miscellaneous.....	318
Troubleshooting.....	319

---

## General Questions

---

### What is KSX II?

KSX II is a second generation digital KVM (Keyboard, Video, Mouse) switch that enables IT administrators to access and control 4 KVM, 4 serial, 8 KVM and 8 serial servers over a network with BIOS-level functionality. KSX II is completely hardware and OS-independent; users can troubleshoot and reconfigure servers even when servers are down.

At the rack, KSX II provides the same functionality, convenience, space savings, and cost savings as traditional analog KVM switches. However, KSX II also integrates the industry's highest-performing serial and KVM-over-IP technology, allowing multiple administrators to access server consoles from any networked workstation.

---

### **How does KSX II differ from remote control software?**

When using KSX II remotely, at first glance, the interface may seem similar to remote control software such as pcAnywhere, Windows Terminal Services / Remote Desktop, VNC, etc. However, because KSX II is not a software but a hardware solution, it's much more powerful:

OS- and hardware-independent - KSX II can be used to manage servers running many popular operating systems, including Intel, Sun, PowerPC running Windows, Linux, Solaris, etc.

State-independent / Agentless - KSX II does not require the managed server OS to be up and running, nor does it require any special software to be installed on the managed server.

Out-of-Band - Even if the managed server's own network connection is unavailable, it can still be managed through KSX II.

BIOS-level access - Even if the server is hung at boot up, requires booting to safe mode, or requires system BIOS parameters to be altered, KSX II still works flawlessly to enable these configurations to be made.

---

### **How do the new features of the KSX II compare to the KSX I?**

KSX II has many new and exciting features, including virtual media, dual gigabit Ethernet, next generation local port, enhanced support for serial ports, etc.

---

### **How do I migrate from the Dominion KSX I to KSX II?**

In general, customers can continue to use their existing switches for many years. As their data centers expand, customers can purchase and use the new KSX II models. Raritan's centralized management appliance, CommandCenter Secure Gateway, and the Multi-Platform Client (MPC) both support KSX I and KSX II switches seamlessly.

---

### **What CIMs are support for the KSX II switch?**

Refer to *Supported Operating Systems and CIMs (KVM Target Servers)* (on page 16).

---

### **Can the KSX II be rack mounted?**

Yes. The KSX II ships standard with 19" rack mount brackets. It can also be reverse rack mounted so the server ports face forward.

---

### How large is the KSX II?

KSX II is only 1U high, fits in a standard 19" rack mount, and is only 11.4" (29 cm) deep.

---

## Serial Access

---

### My Dominion KSX II has just been configured with a network address and I can successfully ping the IP, but when I try to access it using a web browser, the message reads "Page cannot be found or server error, please contact System Administrator."

Check your web browser settings and confirm that a proxy server is being used. If so, click on the checkbox to 'Bypass local addresses or configure DSX IP in the exception list.' Next, make sure the web browser has 128-bit cipher strength. From the Help menu, click on "About" to find this information.

---

### When I select the "Send Break" option from the Emulator menu in Raritan Console (on my DSX), it does not send a break to my Sun server. What could be wrong and how can I address it?

If the SUN machine does not respond to the break signal, verify that the line 'KEYBOARD\_ABORT=disable' is commented out in the /etc/default/kbd file (on the Sun machine). If this line is not commented out, it will disable a keyboard abort sequence; comment out this line to enable the sequence.

---

### How can I consolidate the sites where I have a Dominion KSX II installed?

Raritan's CommandCenter is designed specifically to provide centralized management. It is the ideal solution if you are looking to consolidate management of devices such as Dominion KSX II and other Raritan network-based products.

---

### Is the Ethernet port on the KSX II unit 10/100/1000 Mbps auto sensing?

KSX II supports two 10/100/1000 speed Ethernet interfaces, with configurable speed and duplex settings (either auto-detected or manually set).



---

**Does Dominion KSX II support RS422 and RS485?**

No. Currently Dominion KSX II supports only asynchronous RS232 (also commonly called serial, even though serial is a broad term that covers more than RS232). RS 422 and RS485 are used in industrial automation and other markets. Dominion KSX II is currently designed for connection to serially managed servers and other devices typically found in the data-center and server rooms. This includes serially controlled power strips like Raritan's line of remote power control units.

---

**I have a server/serially managed device that is more than 300 feet from the KSX II - how do I connect?**

You will need to purchase a 3rd party RS232 to RS422/485 converter for each end (two units total) - one at the Dominion end and one connected to the device.

---

**Does Dominion KSX II support RS422 and RS485?**

No. Currently Dominion KSX II supports only asynchronous RS232 (also commonly called serial, even though serial is a broad term that covers more than RS232). RS 422 and RS485 are used in industrial automation and other markets. Dominion KSX II is currently designed for connection to serially managed servers and other devices typically found in the data-center and server rooms. This includes serially controlled power strips like Raritan's line of remote power control units.

---

**Can I open multiple windows and "tile" to monitor multiple servers and other IT equipment?**

Yes, you may monitor and "tile" as many windows as there are serial ports on the Dominion KSX II.

---

**I manage many servers. How do I select a server to connect to?**

From a browser, a simple menu provides the user-assigned name of each server. Users simply click on a server to open a pop-up menu and select Connect from the menu in order to connect to its console port. When using SSH/telnet, the user gets a list of ports they are authorized to connect with when they log in.

---

### **As a user, do I see all servers connected to a Dominion KSX II?**

No. Each user sees only a list of servers they are authorized to manage/view. The administrator of the Dominion KSX II sets up the access privileges to each server.

---

### **Does Dominion KSX II work with Raritan's CommandCenter™?**

Yes, Dominion KSX II is deployable as part of an enterprise-wide management solution with Raritan's CommandCenter™. Hundreds of Dominion KSX II units can be managed via CommandCenter.

---

### **Is the modem used only for administering the Dominion KSX II itself?**

No. Unlike other products in its category, Dominion KSX II offers modem access to administer the box AND get to the target servers.

---

### **Is a modem standard on any Dominion KSX II models?**

Yes, a built-in modem is standard on KSX II models.

---

### **What level of control does Dominion KSX II have over attached target servers?**

The remote user has direct command line access and total control of target devices for maintenance, administration, troubleshooting, and even rebooting. User rights are only restricted by their log-on privileges on Dominion KSX II and the server itself.

---

### **Why do I need to use a serial adapter to connect to some servers?**

While EIA published a standard for RS232 on DB25 and DB9 connectors, there is no standard for RS232 on RJ45. Also, some manufacturers have chosen not to follow the pin out assignments of the EIA on DB25 and DB9 connectors.

---

### **Is the Dominion KSX II unit SUN "break-safe"?**

All Dominion KSX II units are SUN "break-safe" for use with SUN Solaris.

---

**I have lost my Admin password to the Dominion KSX II. Is there a back door or secret password?**

For security reasons, Dominion KSX II does not have any factory default username or password. There is no back-door password. The only option is to restore the unit to its factory default settings and create the Admin username and password again. A hardware reset function to restore the unit to factory default facility is provided.

---

**What remote access connection methods can KSX II accommodate?**

Dominion KSX II provides multiple choices for remote access. These include: Internet, LAN/WAN, or dial-up modem. That means servers can be accessed both in and out of band so remote access to mission critical target servers is always available-even if the network is down.

---

**Which ports need to be open on the corporate firewall for a secure console session using Dominion KSX II?**

Port 443 (for https), port 5000 Discover and Telnet port 23 (this is optional and does not open by default); optionally port 80 (http) for user sessions. For units running software version 2.2 or higher, port 51000 (or other port between 1024-65536). On software releases PRIOR to firmware 2.2 (2.0Bx or 2.1.x) either port 23 or a user-designated port between 2000 and 2400. When using SSH, port 22 needs to be open.

---

**How do I get access to the operating system of the KSX II?**

Dominion KSX II is a secure appliance. Therefore, NO access is possible to the operating system.

---

**I have a few serial devices located a distance away from my server closet and the Dominion KSX II. Can I connect these devices to my Raritan switch?**

Yes. See *Distances for Serial Devices* (on page 270) for more information.

---

**How do I upgrade the software on my Dominion KSX II?**

Use the Firmware Upgrade page to upgrade the firmware for your KSX II unit and all attached D2CIM-VUSB. This page is available in the KSX II Remote Console only.

---

**Are updates to Dominion KSX II software free?**

Yes. Currently all software upgrades are free.

---

**Does Dominion KSX II require any additional client software?**

No. Dominion KSX II is truly "Plug-and-Play" making installation quick and set-up easy. It is not necessary to buy any additional client software or hardware. In addition, no special networking equipment or design is necessary.

---

**What is the name of the terminal emulation package included with Dominion KSX II?**

Raritan Serial Console.

---

**What Authentication mechanisms does the Dominion KSX II support?**

Local database, RADIUS, LDAP/S, Active Directory.

---

**Does Dominion KSX II support SNMP?**

Yes. Dominion KSX II supports SNMP traps via the Raritan Enterprise MIB.

---

**Does Dominion KSX II support syslog?**

Yes. Dominion KSX II supports syslog - to primary and secondary servers.

---

**Can I log every keystroke of a session (input from user and response from a server/device) with a server?**

Yes, KSX II supports client-side logging.

---

**Does Dominion KSX II support TELNET?**

Yes. Dominion KSX II supports enabling of the telnet daemon on the Dominion KSX II unit. Because telnet sends all information "in the clear", enabling telnet is at the customers own discretion, and telnet is disabled by default when the unit ships from the factory. Raritan strongly suggests the use of SSH as a safer alternative to telnet, since all data is encrypted, including the login sequence.

---

**Can I send an intentional "break" signal to the SUN Solaris server when using SSH?**

Yes.

---

**Can I send an intentional "break" signal to the SUN Solaris server when using a web browser?**

Yes, using Raritan Serial Console.

---

**Can I send an intentional "break" signal to the SUN Solaris server when using TELNET?**

Yes.

---

**Can I get the buffered off-line data from a serial port when using SSH?**

Yes.

---

**Can I get the buffered off-line data from a serial port when using telnet?**

Yes.

---

**Can I use KSX II over a VPN connection?**

Yes, KSX II fits into most any network configuration utilizing TCP/IP. KSX II uses standard Internet Protocol (IP) technologies from Layer 1 through Layer 4. Set up the VPN (typically IPSec) connection then start the web-browser and enter the URL for the Dominion unit. The session to the Dominion runs transparently over the VPN tunnel. Traffic can be easily tunneled through standard VPNs.

---

**Can I get the buffered off-line data from a serial port when using a Java-enabled web-browser?**

Yes.

---

**Does Dominion KSX II support local (direct) port access for "crash-cart" applications in a data center?**

Yes.

---

**What are the pin-outs of the Dominion KSX II serial ports?**

To provide maximum port density and to enable simple UTP (Category 5) cabling, 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 following link to find the latest information about the KSX II serial pinouts (RJ-45).

<http://www.raritan.com/support>

---

**What web browsers have you tested with?**

Note that not all web-browsers and SUN JRE behave the same in all languages and operating system versions, so there may be some differences or compatibility issues in some geographies. Some additional testing has been done with Fedora Core 2. Other browsers, for example Mozilla Firefox may work as well, but are not officially tested.

Browser Requirements

Platform	Browser
Netscape 7.0	Win 2K - SUN JRE 1.4.2
Netscape 7.1	Win 2K - SUN JRE 1.4.2
Mozilla 1.5	Win 2K - SUN JRE 1.4.2
Mozilla 1.6	Win 2K - SUN JRE 1.4.2

IE 6.0	Win XP - MS VM
Netscape 7.0	Win XP - SUN JRE 1.4.2
Netscape 7.1	Win XP - SUN JRE 1.4.2
Mozilla 1.5	Win XP - SUN JRE 1.4.2
Mozilla 1.6	Win XP - SUN JRE 1.4.2
Netscape 7.1	RedHat8
Mozilla 1.5	RedHat8
Mozilla 1.6	RedHat8
Netscape 7.1	RedHat9
Mozilla 1.5	RedHat9
Mozilla 1.6	RedHat9
IE 6.0 and 7.0, Netscape 7.0, Netscape 7.1, Mozilla 1.5, Mozilla 1.6	Win 2K - SUN JRE 1.4.2_3
IE 6.0 and 7.0, Netscape 7.0, Netscape 7.1, Mozilla 1.5, Mozilla 1.6	Win XP - SUN JRE 1.4.2_3

---

**The Dominion KSX II uses the web browser to access serial devices. What are the advantages of Java-enabled web browser access?**

For many Solaris/Unix/Linux system administrators, the de facto standard for accessing serial hosts is SSH. However, the SSH clients available for Unix/Linux do not support Apple Macintosh. Additionally, Java-enabled browsers are available on many platforms, including PDAs and handheld PCs. The easy "point-and-click" access offered by Dominion KSX II allows administrators secure access from any Java-enabled web browser.

---

## **Remote Access**

---

---

### **How many users can remotely access servers on each KSX II?**

Up to 8 KVM users can share one KVM channel and up to 8 serial users can share 8 serial channels.

---

### **Can two people look at the same server at the same time?**

Yes, actually up to eight people can access and control any single server at the same time.

---

### **Can two people access the same server, one remotely and one from the local port?**

Yes, the local port is completely independent of the remote "ports." The local port can access the same server using the PC-Share feature.

---

### **In order to access KSX II from a client, what hardware, software or network configuration is required?**

Because KSX II is completely web-accessible, it doesn't require installation of proprietary software on clients used for access. The browser does have to be Java enabled, though.

KSX II can be accessed through major web browsers including: Internet Explorer, Mozilla and Firefox. KSX II can now be accessed on Windows, Linux, Sun Solaris and Macintosh desktops, via Raritan's Java-based Multi-Platform Client (MPC), RSC and the new Virtual KVM Client.

When using an SSH client, the customer has to provide an SSH client. In some operating systems, like Linux, an SSH client is included in the distribution. Also, OpenSSH.org has an SSH client.

KSX II administrators can also perform remote management (set passwords and security, rename servers, change IP address, etc.) using a convenient browser-based interface.



---

**What is the file size of the virtual KVM client applet that is used to access KSX II? How long does it take to retrieve?**

The Virtual KVM Client applet used to access KSX II is approximately 500KB in size. The following chart describes the approximate time required to retrieve KSX II's applet at different network speeds:

100Mbps	Theoretical 100Mbit network speed	0.05 seconds
60Mbps	Likely practical 100Mbit network speed	0.08 seconds
10Mbps	Theoretical 10Mbit network speed	.4 seconds
6Mbps	Likely practical 10Mbit network speed	.8 seconds
512Kbps	Cable modem download speed (typical)	8 seconds

---

**How do I access servers connected to KSX II if the network ever becomes unavailable?**

KSX II offers an internal modem port. With this modem servers can still be remotely accessed in the event of a network emergency. Furthermore, KSX II's local ports always allow access to servers from the rack, regardless of the network condition.

---

**Do you have a non-Windows client?**

Yes. The Virtual KVM Client, Raritan Serial Client (RSC) and the Multi-Platform Client (MPC) allow non-Windows users to connect to KVM target servers through the KSX II switches. MPC can be run via web browsers and standalone.

---

**Sometimes during a Virtual KVM Client session, the Alt key appears to get stuck. What should I do?**

This usually occurs in situations when the Alt key is held and not released. For instance, continuing to press the Alt key while pressing the space bar might cause the focus to change from the target server to the client PC.

The local operating system then interprets this key combination and consequently triggers the action for this key combination in the active window (the client PC).

---

## Universal Virtual Media

---

### What KSX II models support virtual media?

All KSX II models support virtual media. It is available standalone and through CommandCenter Secure Gateway, a centralized management appliance.

---

### What types of virtual media does the KSX II support?

KSX II supports the following types of media: internal and USB-connected CD/DVD drives, USB mass storage devices, PC hard drives, and remote drives.

---

### What is required for virtual media?

The new D2CIM-VUSB CIM is required for virtual media. It supports virtual media sessions to KVM target servers supporting the USB 2.0 interface. Available in economical 32 and 64 quantity CIM packages, this new CIM supports Absolute Mouse Synchronization as well as remote firmware update.

---

### Is virtual media secure?

Yes. Virtual media sessions are secured using 128 BIT AES, 256-bit AES or RC4 encryption.

---

## Ethernet and IP Networking

---

### Does the KSX II offer dual gigabit Ethernet ports to provide redundant fail-over, or load balancing?

Yes. KSX II features dual gigabit Ethernet ports to provide redundant failover capabilities. Should the primary Ethernet port (or the switch/router to which it is connected) fail, KSX II will failover to the secondary network port with the same IP address - ensuring that server operations are not disrupted. Note that automatic failover must be enabled by the administrator.

---

**How much bandwidth does KSX II require?**

KSX II offers next generation KVM-over-IP technology - the very best video compression available. Raritan has received numerous technical awards confirming its high video quality transmissions and the low bandwidth utilization.

Raritan pioneered the KVM-over-IP functionality that allows users to tailor their video parameters to conserve network bandwidth. For instance, when connecting to KSX II through a dial-up modem connection, video transmissions can be scaled to grayscale - allowing users to be fully productive while ensuring high performance.

With that in mind, the following data refers to KSX II at its default video settings - again, these settings can be tailored to a specific environment. They can be increased to provide even higher quality video (color depth), or decreased to optimize for low-speed connections.

As a general rule, a conservative estimate for bandwidth utilization (at KSX II's default settings) is approximately 0.5Mbit/second per active KVM user (connected to and using a server), with very occasional spikes up to 2Mbit/second. This is a very conservative estimate because bandwidth utilization will typically be even lower.

Bandwidth required by each video transmission depends on what task is being performed on the managed server. The more the screen changes, the more bandwidth is utilized. The table below summarizes some use cases and the required bandwidth utilization at KSX II's default settings on a 10Mbit/s network:

Idle Windows Desktop	0 Mbps
Move Cursor Around Desktop	0.18Mbps
Move Static 400x600 Window/Dialog Box	0.35Mbps
Navigate Start Menu	0.49Mbps
Scroll an Entire Page of Text	1.23Mbps
Run 3D Maze Screensaver	1.55Mbps

---

**What is the slowest connection (lowest bandwidth) over which KSX II can operate?**

33Kbps or above is recommended for acceptable KSX II performance over a modem connection.

---

### **What is the speed of KSX II's Ethernet interfaces?**

KSX II supports two 10/100/1000 speed Ethernet interfaces, with configurable speed and duplex settings (either auto-detected or manually set).

---

### **Can I access KSX II over a wireless connection?**

Yes. KSX II not only uses standard Ethernet, but also very conservative bandwidth with very high quality video. Thus, if a wireless client has network connectivity to a KSX II, servers can be configured and managed at BIOS-level wirelessly.

---

### **Can KSX II be used over the WAN (Internet), or just over the corporate LAN?**

Whether via a fast corporate LAN, the less predictable WAN (Internet), cable modem or dial-up modem, KSX II's KVM-over-IP technology can accommodate the connection.

---

### **How many TCP ports must be open on my firewall in order to enable network access to KSX II? Are these ports configurable?**

Only one. KSX II protects network security by only requiring access to a single TCP port to operate. This port is completely configurable for additional security.

Note that, of course, to use KSX II's optional web browser capability, the standard HTTPS port 443 must also be open.

---

### **Can KSX II be used with CITRIX?**

KSX II may work with remote access products like CITRIX if configured appropriately, but Raritan cannot guarantee it will work with acceptable performance. Products like CITRIX utilize video redirection technologies similar in concept to digital KVM switches so that two KVM-over-IP technologies are being used simultaneously.

---

**Does KSX II require an external authentication server to operate?**

No, the KSX II is a completely self-sufficient. After assigning an IP address to a KSX II, it is ready to use - with web browser and authentication capabilities completely built-in.

If an external authentication server (such as LDAP/LDAPS, Active Directory, RADIUS, etc.) is used, KSX II allows this as well, and will even failover to its own internal authentication should the external authentication server become unavailable. In this way, KSX II's design philosophy is optimized to provide ease of installation, complete independence from any external server, and maximum flexibility.

---

**Can the KSX II use DHCP?**

DHCP addressing can be used, however, Raritan recommends fixed addressing since the KSX II is an infrastructure device and can be accessed and administered more effectively with a fixed IP address.

---

**I'm having problems connecting to the KSX II over my IP network. What could be the problem?**

The KSX II relies on your LAN/WAN network. Some possible problems include:

Ethernet auto negotiation. On some networks, 10/100 auto negotiation does not work properly and the KSX II unit must be set to 100MB/full duplex or the appropriate choice for its network.

Duplicate IP Address. If the IP Address of the KSX II is the same as another device, network connectivity may be inconsistent.

Port 5000 conflicts. If another device is using port 5000, the KSX II default port must be changed (or the other device must be changed).

When changing the IP Address of a KSX II, or swapping in a new KSX II, sufficient time must be allowed for its IP and MAC addresses to be known throughout the Layer 2 and Layer 3 networks.

---

## Servers

---

### **Does KSX II depend on a Windows server to operate?**

No. KSX II is completely independent. Even if a user chooses to configure the KSX II to authenticate against an Active Directory server - if that Active Directory server becomes unavailable, KSX II's own authentication will be activated and fully functional.

---

### **Do I need to install a web server such as Microsoft Internet Information Services (IIS) in order to use KSX II's web browser capability?**

No. KSX II is a completely self-sufficient appliance. After assigning an IP address to KSX II, it's ready to use - with web browser and authentication capabilities completely built-in.

---

### **What software do I have to install in order to access KSX II from a particular workstation?**

None. KSX II can be accessed completely via a web browser (although an optional installed client is provided on Raritan's website Raritan.com for the purpose of accessing KSX II via modem). A Java-based client is now available for non-Windows users.

---

## Installation

---

### **Besides the unit itself, what do I need to order from Raritan to install KSX II?**

Each server that connects to KSX II requires a Dominion Computer Interface Module (CIM), a serial cable adapter, and an adapter that connects directly to the keyboard, video, and mouse ports of the server.

---

### **What kind of Cat5 cabling should be used in my installation?**

KSX II can use any standard UTP (unshielded twisted pair) cabling, whether Cat5, Cat5e, or Cat6. Often in our manuals and marketing literature, Raritan will simply say "Cat5" cabling for short. In actuality, any brand UTP cable will suffice for KSX II.

---

**What types of servers can be connected to KSX II?**

KSX II is completely vendor independent. Any server with standard-compliant keyboard, video, and mouse ports can be connected.

---

**How do I connect servers to KSX II?**

See *Connecting to the KSX II* (on page 54).

---

**How far can my servers be from KSX II?**

See *Distances for Serial Devices* (on page 270) and *Target Server Connection Distance and Video Resolution* (on page 270).

---

**Some operating systems lock up when I disconnect a keyboard or mouse during operation. What prevents servers connected to KSX II from locking up when I switch away from them?**

Each Dominion computer interface module (DCIM) dongle acts as a virtual keyboard and mouse to the server to which it is connected. This technology is called KME (keyboard/mouse emulation). Raritan's KME technology is data center grade, battle-tested, and far more reliable than that found in lower-end KVM switches: it incorporates more than 15 years of experience and has been deployed to millions of servers worldwide.

---

**Are there any agents that must be installed on servers connected to KSX II?**

Servers connected to KSX II do not require any software agents to be installed, because KSX II connects directly via hardware to servers' keyboard, video, and mouse ports.

---

**How many servers can be connected to each KSX II unit?**

KSX II models range from 4 to 8 server ports in 1U and 2U chassis. This is the industry's highest digital KVM switch port density.

## Local Port

---

### **What happens if I disconnect a server from KSX II and reconnect it to another KSX II unit, or connect it to a different port on the same KSX II unit?**

KSX II will automatically update the server port names when servers are moved from port to port. This automatic update does not just affect the local access port, but propagates to all remote clients and the optional CommandCenter Secure Gateway management appliance.

Both serial and KVM ports can be moved without encountering problems. However, once disconnected, the name of a KVM will be retained but the name for a serial port will not be.

---

## Local Port

---

### **Can I access my servers directly from the rack?**

Yes. At the rack, KSX II functions just like a traditional KVM switch - allowing control of up to 16 servers using a single keyboard, monitor, and mouse.

---

### **When I am using the local port, do I prevent other users from accessing servers remotely?**

No. The KSX II local port has a completely independent access path to the servers. This means a user can access servers locally at the rack - without compromising the number of users that access the rack remotely at the same time.

---

### **Can I use a USB keyboard or mouse at the local port?**

Yes. KSX II offers both PS/2 and USB keyboard and mouse ports on the local port. Note that the USB ports are USB v1.1, and support keyboards and mice only - not USB devices such as scanners or printers.

---

### **Is there an On-Screen Display (OSD) for local, at-the-rack access?**

Yes, but KSX II's at-the-rack access goes way beyond conventional OSDs. Featuring the industry's first browser-based interface for at-the-rack access, KSX II's local port uses the same interface for local and remote access. Moreover, most administrative functions are available at-the-rack.



---

**How do I select between servers while using the local port?**

The local port displays the connected servers using the same user interface as the remote client. Connect to a server with a simple click of the mouse.

---

**How do I ensure that only authorized users can access servers from the local port?**

Users attempting to use the local port must pass the same level of authentication as those accessing remotely. This means that:

- If the KSX II is configured to interact with an external RADIUS, LDAP/LDAPS or Active Directory server, users attempting to access the local port will authenticate against the same server.
- If the external authentication servers are unavailable, KSX II fails-over to its own internal authentication database.
- KSX II has its own standalone authentication, enabling instant, out-of-the-box installation.

---

**If I use the local port to change the name of a connected server, does this change propagate to remote access clients as well? Does it propagate to the optional CommandCenter appliance?**

Yes. The local port presentation is identical and completely in sync with remote access clients, as well as Raritan's optional CommandCenter Secure Gateway management appliance. To be clear, if the name of a server via the KSX II on-screen display is changed, this updates all remote clients and external management servers in real-time.

---

**If I use KSX II's remote administration tools to change the name of a connected server, does that change propagate to the local port as well?**

Yes. The local port presentation is identical and completely in sync with remote access clients. To be clear, if the name of a server via the KSX II on-screen display is changed, this updates all remote clients and external management servers in real-time.

## Power Control

---

### **Sometimes I see "shadows" on the local port user interface. Why does that occur?**

This shadow/ghosting effect may occur with LCD monitors that have been on for long periods. The LCD properties and the electrical/static charge can produce these effects when the screen is on for a long time.

---

## Power Control

---

### **Does the power supply used by KSX II automatically detect voltage settings?**

Yes. KSX II's power supply can be used in AC voltage ranges from 100-240 volts, at 50-60 Hz.

---

### **What type of power control capabilities does KSX II offer?**

Raritan's Remote Power Control power strips can be connected to the KSX II to provide power control of the KVM target servers. 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 reinserting the plug.

---

### **Does KSX II support servers with multiple power supplies? What if each power supply is connected to a different power strip?**

Yes. KSX II can be easily configured to support multiple power supplies connected to multiple power strips. Two (2) power strips can be connected to a KSX II device. Four power supplies can be connected per target server to multiple power strips.

---

### **Does remote power control require any special server configuration?**

Some servers ship with default BIOS settings such that the server does not automatically restart after losing and regaining power. See the server user manual for more information.

---

### **What type of power strips does KSX II support?**

To take advantage of KSX II's integrated power control user interface and, more importantly, integrated security, use Raritan's Remote Power Control (RPC) power strips or Dominion PX power strips.

RPCs come in many outlet, connector, and amp variations. The D2CIM-PWR must be purchased to connect the RPC to the KSX II.

The Dominion PX is an intelligent power distribution unit that allows you to reboot remote servers and other network devices, and monitor power in the data center, through Raritan's KVM switches and Secure Console Servers.

---

## **Scalability**

---

### **How do I connect multiple KSX II devices together into one solution?**

Multiple KSX II units do not need to be physically connected together. Instead, each KSX II unit connects to the network, and they automatically work together as a single solution if deployed with Raritan's optional CommandCenter Secure Gateway (CC-SG) management appliance. CC-SG acts as a single access point for remote access and management. CC-SG offers a significant set of convenient tools, such as consolidated configuration, consolidated firmware update, and a single authentication and authorization database.

In addition, CC-SG enables sophisticated server sorting, permissions, and access. If deployment of Raritan's CC-SG management appliance isn't an option, multiple KSX II units still interoperate and scale automatically: The KSX II's remote user interface and the Multi-Platform Client will automatically discover KSX II units. Non-discovered KSX II units can be accessed via a user-created profile.

---

### **Can I connect an existing analog KVM switch to KSX II?**

Yes. Analog KVM switches can be connected to one of KSX II's server ports. Simply use a PS/2 Computer Interface Module (CIM), and attach it to the user ports of the existing analog KVM switch. Please Note that analog KVM switches vary in their specifications and Raritan cannot guarantee the interoperability of any particular third-party analog KVM switch. Contact Raritan technical support for further information.

---

## Security

---

### **What kind of encryption does KSX II use?**

KSX II uses industry-standard (and extremely secure) 128-bit RC4, 128 bit AES or 256bit AES encryption, both in its SSL communications as well as its own data stream. Literally no data is transmitted between remote clients and KSX II that is not completely secured by encryption.

---

### **Does KSX II support AES encryption as recommended by the US Government's NIST and FIPs standards?**

The KSX II utilizes the Advanced Encryption Standard (AES) encryption for added security.

AES is a US government approved cryptographic algorithm that is recommended by the National Institute of Standards and Technology (NIST) in the FIPS Standard 197.

---

### **Does KSX II allow encryption of video data? Or does it only encrypt keyboard and mouse data?**

Unlike competing solutions, which only encrypt keyboard and mouse data, KSX II does not compromise security - it allows encryption of keyboard, mouse and video data.

---

### **How does KSX II integrate with external authentication servers such as Active Directory, RADIUS, or LDAP/S?**

Through a very simple configuration, KSX II can be set to forward all authentication requests to an external server such as LDAP/S, Active Directory, or RADIUS. For each authenticated user, KSX II receives from the authentication server the user group to which that user belongs. KSX II then determines the user's access permissions depending on the user group to which he or she belongs.

---

### **How are usernames and passwords stored?**

Should KSX II's internal authentication capabilities be used, all sensitive information such as usernames and passwords are stored in an encrypted format. Literally no one, including Raritan technical support or Product Engineering departments, can retrieve those usernames and passwords.

---

**Does KSX II support strong password?**

Yes. The KSX II has administrator-configurable, strong password checking to ensure that user-created passwords meet corporate and/or government standards and are resistant to brute force hacking.

---

**If the KSX II Encryption Mode is set to Auto, what level of encryption is achieved?**

KSX II has the ability to support AES-256. For this to happen, Java unlimited strength policy files have to be loaded on the client machine. Once this is enabled, the encryption level that is auto-negotiated when the mode is set to AUTO is as follows:

Browser	Encryption Level
Internet Explorer 6	AES-128
Internet Explorer 7	AES-256
Firefox 1.5	AES-256
Firefox 2.0	AES-256
Mozilla 1.7	AES-256
Safari 2.0.4	AES-256

---

**Manageability**

---

**Can KSX II be remotely managed and configured via web browser?**

Yes. KSX II can be completely configured remotely via web browser. Note that this does require that the workstation have an appropriate Java Runtime Environment (JRE) version installed.

Besides the initial setting of KSX II's IP address, everything about the solution can be completely set up over the network. (In fact, using a crossover Ethernet cable and KSX II's default IP address, you can even configure the initial settings via web browser.)

## Miscellaneous

---

### **Can I backup and restore KSX II's configuration?**

Yes. KSX II's device and user configurations can be completely backed up for later restoration in the event of a catastrophe.

KSX II's backup and restore functionality can be used remotely over the network, or through a web browser.

---

### **What auditing or logging does KSX II offer?**

For complete accountability, KSX II logs all major user events with a date and time stamp. For instance, reported events include (but are not limited to): user login, user logout, user access of a particular server, unsuccessful login, configuration changes, etc.

---

### **Can KSX II integrate with Syslog?**

Yes. In addition to KSX II's own internal logging capabilities, KSX II can send all logged events to a centralized Syslog server.

---

### **Can KSX II integrate with SNMP?**

Yes. In addition to KSX II's own internal logging capabilities, KSX II can send SNMP traps to SNMP management systems like HP Openview and Raritan's CC-NOC.

---

### **Can KSX II's internal clock be synchronized with a timeserver?**

Yes. KSX II supports the industry-standard NTP protocol for synchronization with either a corporate timeserver, or with any public timeserver (assuming that outbound NTP requests are allowed through the corporate firewall).

---

## Miscellaneous

---

### **What is KSX II's default IP address?**

192.168.0.192

---

**What is KSX II's default username and password?**

The KSX II's default username and password are admin/raritan [all lower case]. However, for the highest level of security, the KSX II forces the administrator to change the KSX II default administrative username and password when the unit is first booted up.

---

**I changed and subsequently forgot KSX II's administrative password; can you retrieve it for me? (Share)**

KSX II contains a hardware reset button that can be used to factory reset the device, which will reset the administrative password on the device.

---

## Troubleshooting

---

**I am logged into the KSX II using Firefox, and I opened another Firefox browser. I am automatically logged into the same KSX II with the second Firefox browser. Is this right?**

Yes, this is correct behavior and is the direct result of how browsers and cookies function.

---

**I am logged into the KSX II using Firefox and I attempt to log into another KSX II using another Firefox browser session from the same client. I am logged out of both KSX IIs; is this correct behavior?**

Yes, to access two different KSX II devices, either close the first session, or use another client PC.





# Index

## 1

1. AC Power • 34

## 2

2. Network Ports • 34

## 3

3. Local User Port (local PC) and Local Admin Port • 35

## 4

4. KVM Target Server Ports • 35

## 5

5. Power Strip • 36

## 6

6. Serial Target Ports • 36

## A

About Raritan Virtual KVM Client • 104

Absolute • 21, 101

Accessing a Target Server • 201

Accessing Target Servers • 72

Accessing the KSX II Using CLI • 235

Add New Favorite • 70

Add New User Group • 122, 123

Adding a New User • 120

Adding Attributes to the Class • 280

Administering the KSX II Console Server Configuration Commands • 245

AES\_256 Support for Java Clients • 287

Apple Macintosh Settings • 32

Are there any agents that must be installed on servers connected to KSX II? • 312

Are updates to Dominion KSX II software free? • 301

As a user, do I see all servers connected to a Dominion KSX II? • 299

Assign a Name to the PX • 162

Assign an IP Address • 39

Associate KVM and Serial Target Servers to Outlets (Port Page) • 163

Audit Log • 180, 198, 206

Authentication Settings • 132

Authentication vs. Authorization • 49

Auto-sense Video Settings • 95

Available Resolutions • 200

## B

Backup and Restore • 182

Besides the unit itself, what do I need to order from Raritan to install KSX II? • 311

## C

Calibrate Color • 96

Can I access KSX II over a wireless connection? • 309

Can I access my servers directly from the rack? • 313

Can I backup and restore KSX II's configuration? • 319

Can I connect an existing analog KVM switch to KSX II? • 316

Can I get the buffered off-line data from a serial port when using a Java-enabled web-browser? • 302

Can I get the buffered off-line data from a serial port when using SSH? • 302

Can I get the buffered off-line data from a serial port when using telnet? • 302

Can I log every keystroke of a session (input from user and response from a server/device) with a server? • 301

Can I open multiple windows and • 298

Can I send an intentional • 302

Can I use a USB keyboard or mouse at the local port? • 313

Can I use KSX II over a VPN connection? • 302

Can KSX II be remotely managed and configured via web browser? • 318

Can KSX II be used over the WAN (Internet), or just over the corporate LAN? • 309

## Index

- Can KSX II be used with CITRIX? • 309
  - Can KSX II integrate with SNMP? • 319
  - Can KSX II integrate with Syslog? • 319
  - Can KSX II's internal clock be synchronized with a timeserver? • 319
  - Can the KSX II be rack mounted? • 296
  - Can the KSX II use DHCP? • 310
  - Can two people access the same server, one remotely and one from the local port? • 305
  - Can two people look at the same server at the same time? • 305
  - I changed and subsequently forgot KSX II's administrative password • 320
  - CC Unmanage • 248
  - CC-SG • 294
  - CD-ROM/DVD-ROM/ISO Images • 110, 114, 116
  - Certified Modems for UNIX, Linux and MPC • 251
  - Change Password • 131
  - Change the Keyboard Layout Code (Sun Targets) • 32
  - Changing the Default Password • 38
  - Chat • 232
  - Checking Your Browser for AES Encryption • 174, 176
  - CIM Upgrade • 184
  - CIMs • 293
  - CLI Commands • 243
  - CLI Prompts • 243
  - CLI Syntax -Tips and Shortcuts • 241
  - Client Dial-Up Networking Configuration • 251
  - Command Line Interface (CLI) • 234
  - Common Commands for all Command Line Interface Levels • 241
  - Completion of Command • 240
  - Computer Interface Modules (CIMs) • 266
  - Conditions when Read-Write is not Available • 112, 113
  - Configure Direct Port Access • 40
  - Configure KVM and Serial Ports • 42
  - Configuring Network • 245
  - Connect Commands • 247
  - Connect the Dominion PX • 159
  - Connecting to a KVM Target Server • 76
  - Connecting to a Serial Target Server • 77
  - Connecting to the KSX II • 54, 312
  - Connecting to Virtual Media • 112
  - Connection • 89
  - Connection Menu • 87
  - Connectivity • 267, 273
  - Creating a Keyboard Macro • 92
  - Creating a New Attribute • 279
- ## D
- Date/Time Settings • 149
  - DB25F Nulling Serial Adapter Pinouts • 275
  - DB25M Nulling Serial Adapter Pinouts • 276
  - DB9F Nulling Serial Adapter Pinouts • 275
  - DB9M Nulling Serial Adapter Pinouts • 275
  - Default IP Address • 15
  - Default RSC Option Values • 219
  - Dell OpTipler and Dimension Computers • 293
  - Desktop Background • 20
  - Device Diagnostics • 195
  - Device Information • 181
  - Device Management • 141, 236
  - Device Services • 146
  - Device Settings Menu • 141
  - Diagnostics • 189
  - Diagnostics Menu • 189
  - Disconnecting KVM and Serial Targets • 77
  - Disconnecting Virtual Media • 110, 115
  - Discover Devices - KSX II Subnet • 69
  - Discover Devices - Local Subnet • 67
  - Distances for Serial Devices • 270, 300, 312
  - Do I need to install a web server such as Microsoft Internet Information Services (IIS) in order to use KSX II's web browser capability? • 311
  - Do you have a non-Windows client? • 306
  - Does Dominion KSX II require any additional client software? • 301
  - Does Dominion KSX II support local (direct) port access for • 302
  - Does Dominion KSX II support RS422 and RS485? • 298
  - Does Dominion KSX II support SNMP? • 301

- Does Dominion KSX II support syslog? • 301
- Does Dominion KSX II support TELNET? • 301
- Does Dominion KSX II work with Raritan's CommandCenter™? • 299
- Does KSX II allow encryption of video data? Or does it only encrypt keyboard and mouse data? • 317
- Does KSX II depend on a Windows server to operate? • 311
- Does KSX II require an external authentication server to operate? • 310
- Does KSX II support AES encryption as recommended by the US Government's NIST and FIPs standards? • 317
- Does KSX II support servers with multiple power supplies? What if each power supply is connected to a different power strip? • 315
- Does KSX II support strong password? • 318
- Does remote power control require any special server configuration? • 315
- Does the KSX II offer dual gigabit Ethernet ports to provide redundant fail-over, or load balancing? • 307
- Does the power supply used by KSX II automatically detect voltage settings? • 315
- Dominion KSX II Overview • 2

## E

- Edit • 228
- Editing rcusergroup Attributes for User Members • 282
- Electrical Specifications • 267
- Emergency Connectivity • 267
- Emulator • 219
- Enabling Telnet • 237
- Encryption & Share • 173
- Environmental Requirements • 265
- Ethernet and IP Networking • 307
- Event Management • 150
- Event Management - Destinations • 153
- Event Management - Settings • 151
- Exit • 90
- External Product Overview • 9

## F

- Factory Reset (KSX II Local Console Only) • 206
- FAQs • 295
- Favorites List • 65
- File Server Setup (File Server ISO Images Only) • 109, 116
- Firmware Upgrade • 185
- French Keyboard • 288
- From LDAP • 277
- From Microsoft Active Directory • 278

## G

- General Questions • 295
- Getting Started • 15, 242
- Group-based IP ACL (Access Control List) • 125, 126, 131, 146, 176
- Groups • 52

## H

- Hardware • 6
- Help • 232
- Help Menu • 104
- Hotkeys • 76, 77, 201
- How are usernames and passwords stored? • 317
- How can I consolidate the sites where I have a Dominion KSX II installed? • 297
- How do I access servers connected to KSX II if the network ever becomes unavailable? • 306
- How do I connect multiple KSX II devices together into one solution? • 316
- How do I connect servers to KSX II? • 312
- How do I ensure that only authorized users can access servers from the local port? • 314
- How do I get access to the operating system of the KSX II? • 300
- How do I migrate from the Dominion KSX I to KSX II? • 296
- How do I select between servers while using the local port? • 314
- How do I upgrade the software on my Dominion KSX II? • 300

## Index

- How do the new features of the KSX II compare to the KSX I? • 296
- How does KSX II differ from remote control software? • 296
- How does KSX II integrate with external authentication servers such as Active Directory, RADIUS, or LDAP/S? • 317
- How far can my servers be from KSX II? • 312
- How large is the KSX II? • 297
- How many servers can be connected to each KSX II unit? • 312
- How many TCP ports must be open on my firewall in order to enable network access to KSX II? Are these ports configurable? • 309
- How many users can remotely access servers on each KSX II? • 305
- How much bandwidth does KSX II require? • 308
- I**
- I am logged into the KSX II using Firefox, and I opened another Firefox browser. I am automatically logged into the same KSX II with the second Firefox browser. Is this right? • 320
- I have a few serial devices located a distance away from my server closet and the Dominion KSX II. Can I connect these devices to my Raritan switch? • 300
- I have a server/serially managed device that is more than 300 feet from the KSX II - how do I connect? • 298
- I have lost my Admin password to the Dominion KSX II. Is there a back door or secret password? • 300
- I manage many servers. How do I select a server to connect to? • 298
- IBM AIX 5.3 Settings • 31
- If I use KSX II's remote administration tools to change the name of a connected server, does that change propagate to the local port as well? • 314
- If I use the local port to change the name of a connected server, does this change propagate to remote access clients as well? Does it propagate to the optional CommandCenter appliance? • 314
- If the KSX II Encryption Mode is set to Auto, what level of encryption is achieved? • 318
- I'm having problems connecting to the KSX II over my IP network. What could be the problem? • 310
- Implementing LDAP Remote Authentication • 132, 135, 137
- Implementing RADIUS Remote Authentication • 132, 138
- In order to access KSX II from a client, what hardware, software or network configuration is required? • 305
- Informational Notes • 56, 286
- Initial Configuration • 242
- Installation • 311
- Installation and Configuration • 19, 86
- Installing RSC for Sun Solaris and Linux • 215
- Installing RSC on Windows • 213
- Intelligent • 21, 101
- Interface Command • 246
- Introduction • 1
- IP Access Control • 125, 127, 146, 176
- Is a modem standard on any Dominion KSX II models? • 299
- Is the Dominion KSX II unit SUN • 299
- Is the Ethernet port on the KSX II unit 10/100/1000 Mbps auto sensing? • 297
- Is the modem used only for administering the Dominion KSX II itself? • 299
- Is there an On-Screen Display (OSD) for local, at-the-rack access? • 313
- I am logged into the KSX II using Firefox and I attempt to log into another KSX II using another Firefox browser session from the same client. I am logged out of both KSX IIs • 320
- Is virtual media secure? • 307

## J

- Java Runtime Environment (JRE) • 57, 290

**K**

- Keyboard Language Preference (Fedora Linux Clients) • 290
- Keyboard Macros • 91
- Keyboard Menu • 90
- KSX II Console Layout • 59
- KSX II Console Menus • 59
- KSX II Local Console • 197
  - KSX II Devices • 55, 200
- KSX II Local Console Interface • 200
- KSX II Serial RJ-45 Pinouts • 274
- KVM Properties • 268

**L**

- LAN Interface Settings • 145
- Language Support • 56
- Launching RSC from a KSX II Remote Console • 216
- Launching the KSX II • 57
- Linux Settings (Red Hat 4) • 26
- Linux Settings (Red Hat 9) • 24
- Local Drives • 109, 112
- Local Port • 313
- Local Port Administration • 202
- Local Port Settings (KSX II Local Console Only) • 55, 201, 202, 203
- Local Serial Port Connection to the KSX II • 237
- Logging Out • 62
- Login • 238
- Login Information • 15
- Login Limitations • 168, 170

**M**

- Macintosh Keyboard • 286, 291
- Maintenance • 179
- Maintenance Features (Local/Remote Console) • 179
- Maintenance Menu • 179
- Make Linux Settings Permanent • 27
- Make UNIX Settings Permanent • 28
- Manageability • 318
- Managing Favorites • 61, 62
- Menu Tree • 83

- Miscellaneous • 319
- Modem Configuration • 10, 251
- Modem Settings • 148
- Modify Existing User • 119, 121
- Modify Existing User Group • 129
- Modifying a Keyboard Macro • 94
- Mouse Menu • 85, 99
- Mouse Pointer Synchronization • 85
- Mouse Pointer Synchronization (Fedora) • 291
- Mouse Settings • 21
- Mouse Synchronization Tips • 85
- Multi-Platform Client (MPC) • 55
- My Dominion KSX II has just been configured with a network address and I can successfully ping the IP, but when I try to access it using a web browser, the message reads • 297

**N**

- Name Command • 246
- Navigation of the CLI • 240
- Network Basic Settings • 143
- Network Interface Page • 190
- Network Settings • 142
- Network Speed Settings • 146, 272
- Network Statistics Page • 190
- Non-US Keyboards • 286, 288
- Note on Microsoft Active Directory • 48
- Note to CC-SG Users • 48

**O**

- Opening a KVM Session • 110
- Operating System Mouse and Video Settings • 21
- Options • 83, 102
- Organization of Information • 13
- Overview • 19, 82, 106, 234, 248, 286

**P**

- Package Contents • 12
- Physical Connections • 198
- Physical Specifications • 266
- Ping Host Page • 193
- Port Access Page • 73
- Port Action Menu - KVM and Serial Ports • 75



## Index

Port Configuration Page • 158  
Port Keywords • 48, 165  
Port Settings • 238  
Port Sharing Using CLI • 245  
Power Control • 10, 159, 315  
Power Controlling a Target Server • 78  
Power Cycle a Target Server • 78  
Power Off a Target Server • 80  
Power On a Target Server • 79  
Prerequisites for Using Virtual Media • 108, 109  
Product Features • 6  
Product Photos • 5  
Properties Dialog • 87  
Proxy Mode and MPC • 294

## R

RADIUS Communication Exchange Specifications • 139  
Raritan Serial Client Interface • 217  
Raritan Serial Console • 208  
Reboot • 187  
Refresh Screen • 95  
Related Documentation • 14  
Relationship between Users and Groups • 53  
Remote Access • 305  
Remote Authentication • 48, 205  
Remote Connection • 268  
Removing a Keyboard Macro • 94  
Removing KSX II from CC-SG Management • 249  
Reset Button • 10, 175, 198  
Resolving Fedora Core Focus • 292  
Returning to the KSX II Local Console Interface • 202  
Returning User Group Information • 277  
Returning User Group Information from Active Directory Server • 137  
Returning User Group Information via RADIUS • 139  
Running a Keyboard Macro • 94

## S

Scalability • 316  
Scaling • 103

Security • 317  
Security and Authentication • 199  
Security Issues • 244  
Security Settings • 120, 168  
Security Settings Menu • 169  
Send Ctrl+Alt+Delete • 90  
Serial Access • 297  
Server Display • 200  
Servers • 311  
Set CIM Keyboard/Mouse Options • 90  
Set Emulation on Target • 244  
Set Permissions for Individual Group • 121, 131  
Setting Linux OS Variables • 212  
Setting Network Parameters • 242  
Setting Parameters • 242  
Setting Permissions • 125  
Setting Port Permissions • 126  
Setting the Registry to Permit Write Operations to the Schema • 278  
Setting UNIX OS Variables • 212  
Setting Windows OS Variables • 208  
Simultaneous Users • 199  
Single Mouse Cursor • 100  
Software • 7  
Some operating systems lock up when I disconnect a keyboard or mouse during operation. What prevents servers connected to KSX II from locking up when I switch away from them? • 312  
Sometimes during a Virtual KVM Client session, the Alt key appears to get stuck. What should I do? • 306  
Sometimes I see • 315  
Specifications • 35, 265  
SSH Access from a UNIX Workstation • 236  
SSH Access from a Windows PC • 236  
SSH Connection to the KSX II • 236  
Standard • 21, 100  
Starting the KSX II Local Console • 199  
Step 1  
    Configure KVM Target Servers • 19, 99  
Step 2 (Optional)  
    Configure Keyboard Language • 32  
Step 3

- Configure Network Firewall Settings • 33
- Step 4
  - Connect the Equipment • 10, 11, 34, 42
- Step 5
  - KSX II Initial Configuration • 38
- Strong Passwords • 132, 168, 171
- Sun Solaris Settings • 28
- Supported Browsers • 16
- Supported Operating Systems (Clients) • 8, 15
- Supported Operating Systems and CIMs (KVM Target Servers) • 16, 296
- Supported Protocols • 48
- Supported Video Resolutions • 20
- SUSE Linux 10.1 Settings • 26
- SUSE/VESA Video Modes • 292
- Switching Between KVM Target Servers • 77
- Synchronize Mouse • 99
- System Requirements • 208

## T

- Target BIOS Boot Time with Virtual Media • 293
- Target Connections and the CLI • 244
- Target Screen Resolution • 104
- Target Server Connection Distance and Video Resolution • 20, 85, 270, 312
- TCP and UDP Ports Used • 269
- TELNET Access from a Windows PC • 237
- Telnet Connection to the KSX II • 236
- Terminology • 7
- The Dominion KSX II uses the web browser to access serial devices. What are the advantages of Java-enabled web browser access? • 304
- Toolbar • 84
- Tools • 229
- Tools Menu • 102
- Trace Route to Host Page • 194
- Troubleshooting • 320

## U

- Universal Virtual Media • 307
- Updating the LDAP/LDAPS Schema • 277
- Updating the Schema Cache • 281
- Upgrade History • 187

- User Blocking • 168, 172
- User Group List • 122
- User Guide • 12
- User Interfaces • 54
- User List • 119
- User Management • 118
- User Management Menu • 118
- Users • 52
- Users, Groups, and Access Permissions • 53
- Users, Groups, Relationships and Access Permissions • 52
- Using Virtual Media • 109

## V

- Video Menu • 95
- Video Settings • 96
- View Menu • 103
- View Toolbar • 103
- Virtual KVM Client • 75, 76, 77, 81, 111
- Virtual KVM Client Version not Known from CC-SG Proxy Mode • 294
- Virtual Media • 4, 101, 105, 293
- Virtual Media not Refreshed after Files Added • 293

## W

- What are the pin-outs of the Dominion KSX II serial ports? • 303
- What auditing or logging does KSX II offer? • 319
- What Authentication mechanisms does the Dominion KSX II support? • 301
- What CIMs are support for the KSX II switch? • 296
- What happens if I disconnect a server from KSX II and reconnect it to another KSX II unit, or connect it to a different port on the same KSX II unit? • 313
- What is KSX II? • 295
- What is KSX II's default IP address? • 319
- What is KSX II's default username and password? • 320
- What is required for virtual media? • 307

## Index

- What is the file size of the virtual KVM client applet that is used to access KSX II? How long does it take to retrieve? • 306
- What is the name of the terminal emulation package included with Dominion KSX II? • 301
- What is the slowest connection (lowest bandwidth) over which KSX II can operate? • 308
- What is the speed of KSX II's Ethernet interfaces? • 309
- What kind of Cat5 cabling should be used in my installation? • 311
- What kind of encryption does KSX II use? • 317
- What KSX II models support virtual media? • 307
- What level of control does Dominion KSX II have over attached target servers? • 299
- What remote access connection methods can KSX II accommodate? • 300
- What software do I have to install in order to access KSX II from a particular workstation? • 311
- What type of power control capabilities does KSX II offer? • 315
- What type of power strips does KSX II support? • 316
- What types of servers can be connected to KSX II? • 312
- What types of virtual media does the KSX II support? • 307
- What web browsers have you tested with? • 303
- When I am using the local port, do I prevent other users from accessing servers remotely? • 313
- When I select the • 297
- Which ports need to be open on the corporate firewall for a secure console session using Dominion KSX II? • 300
- Why do I need to use a serial adapter to connect to some servers? • 299
- Windows 2000 Dial-Up Networking Configuration • 254
- Windows 2000 Settings • 22
- Windows 3-Button Mouse on Linux Targets • 293
- Windows NT Dial-Up Networking Configuration • 251
- Windows Vista • 23
- Windows XP / Windows 2003 Settings • 21
- Windows XP Dial-Up Networking Configuration • 258





➤ **U.S./Canada/Latin America**

Monday - Friday  
8 a.m. - 8 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, China**

Monday - Friday  
9 a.m. - 6 p.m. local time  
Phone: +86-10-88091890

**Shanghai, China**

Monday - Friday  
9 a.m. - 6 p.m. local time  
Phone: +86-21-5425-2499

**GuangZhou, China**

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

➤ **Korea**

Monday - Friday  
9 a.m. - 6 p.m. local time  
Phone: +82-2-5578730

➤ **Taiwan**

Monday - Friday  
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight  
Phone: +886-2-8919-1333  
Email: tech.rap@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+1 CET  
Phone +44-20-7614-77-00

**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 p.m. GMT+1 CET  
Phone: +49-20-17-47-98-0

➤ **Japan**

Monday - Friday  
9:30 a.m. - 5:30 p.m. local time  
Phone: +81-3-3523-5994  
Email: support.japan@raritan.com

➤ **Melbourne, Australia**

Monday - Friday  
9:00 a.m. - 6 p.m. local time  
Phone: +61-3-9866-6887

