



KX II-101

User Guide 2.0.20

Copyright © 2008 Raritan, Inc.

KX2101-v2.20-0B-E

July 2008

255-62-4031-00

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 2008 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

What's New in the User Guide.....	1
KX II-101 Overview	2
Product Photos	4
Product Features	5
Interfaces	5
Network Configuration	5
System Management Features	5
Administration Features.....	5
User Features.....	6
Power.....	6
Video Resolution	6
Mounting	6
Terminology	6
Package Contents.....	7
Optional Accessories	7
User Guide	7
Related Documentation	8

Chapter 2 Installation and Configuration 9

Overview	9
Default Logon Information	9
Getting Started.....	10
Step 1: Configure the Target Server.....	10
Step 2: Configure Network Firewall Settings.....	16
Step 3: Connect the KX II-101.....	17
Step 4: Configure the KX II-101.....	24

Chapter 3 Working with Target Servers 32

Interfaces	32
KX II-101 Remote Console Interface.....	32
Multi-Platform Client Interface	41
Virtual KVM Client.....	41
Overview.....	41
Connecting to a KVM Target Server	41
VKC Toolbar	42
Power Controlling a KVM Target Server	42
Disconnecting a KVM Target Server	43
VKC Connection Properties.....	43
Connection Information	45

Keyboard Options.....	46
Video Properties	49
Mouse Options.....	52
VKC Virtual Media	56
Tool Options	57
View Options.....	59
Help Options	59
Multi-Platform Client (MPC)	60
Requirements and Installation	60
Operation	60
Administrative Functions	99

Chapter 4: Virtual Media 106

Overview	107
Prerequisites for Using Virtual Media	110
File Server Setup (File Server ISO Images Only).....	111
Connecting to Virtual Media.....	113
Local Drives	113
Conditions when Read/Write is Not Available.....	114
CD-ROM/DVD-ROM/ISO Images.....	114
Disconnecting Virtual Media	115

Chapter 5 User Management 116

User Groups.....	116
User Group List.....	117
Relationship Between Users and Groups	117
Adding a New User Group.....	118
Modifying an Existing User Group.....	123
Users.....	123
User List.....	124
Adding a New User.....	124
Modifying an Existing User	125
Blocking and Unblocking Users.....	125
Authentication Settings	126
Implementing LDAP/LDAPS Remote Authentication	127
Returning User Group Information from Active Directory Server	129
Implementing RADIUS Remote Authentication.....	130
Returning User Group Information via RADIUS.....	133
RADIUS Communication Exchange Specifications.....	133
User Authentication Process	135
Changing a Password.....	137

Chapter 6 Device Management 138

Network Settings.....	138
Network Basic Settings.....	139
LAN Interface Settings.....	140

Device Services	141
Keyboard/Mouse Setup	143
Serial Port Settings	144
Admin Port	144
Raritan Power Strip Control	145
Modem	146
Date/Time Settings	148
Event Management	149
Configuring Event Management - Settings	150
Event Management - Destinations	151
Port Configuration	154
Managing KVM Target Servers (Port Page)	155
Power Control	157

Contents

Analog KVM Switch	162
Resetting the KX II-101 Using the Reset Button	163

Chapter 7 Managing USB Connections 165

Overview	166
Basic USB Connection Settings	166
Advanced USB Connection Settings	168
Known USB Profiles.....	169

Chapter 8 Security Management 184

Security Settings	184
Logon Limitations.....	185
Strong Passwords.....	186
User Blocking.....	188
Encryption & Share.....	190
Checking Your Browser for AES Encryption	192
IP Access Control	193

Chapter 9 Maintenance 195

Audit Log.....	195
Device Information.....	196
Backup and Restore	197
Upgrading Firmware	198
Upgrade History	200
Rebooting.....	201

Chapter 10 Diagnostics 202

Network Interface Page	202
Network Statistics Page.....	203
Ping Host Page.....	206
Trace Route to Host Page	206
Device Diagnostics	208

Chapter 11 Command Line Interface (CLI) 210

Overview	210
Accessing the KX II-101 Using the CLI.....	211
SSH Connection to the KX II-101	211
SSH Access from a Windows PC.....	211
SSH Access from a UNIX/Linux Workstation	212
Logging On	212
Navigation of the CLI	212
CLI Prompts.....	213
Completion of Commands	213

CLI Syntax -Tips and Shortcuts.....	214
Common Commands for All Command Line Interface Levels	214
CLI Commands	214
Diagnostics	215
Configuration	216
Listports Command	218
Userlist Command	218
Chapter 12 CC Unmanage	219
Overview	219
Removing a KX II-101 from CC-SG Management.....	220
Using CC-SG in Proxy Mode	221
Appendix A Specifications	222
KX II-101 Specifications.....	222
Supported Video Resolutions	223
Supported Keyboard Languages	224
Supported Operating Systems (Clients)	225
Supported Browsers	225
Certified Modems.....	226
Connectors.....	226
TCP and UDP Ports Used	226
Network Speed Settings	228
Admin Port Pinout Information.....	229
9 Pin Pinout.....	230
Appendix B Updating the LDAP Schema	231
Returning User Group Information.....	231
From LDAP	231
From Microsoft Active Directory	231
Setting the Registry to Permit Write Operations to the Schema	232
Creating a New Attribute.....	232
Adding Attributes to the Class	233
Updating the Schema Cache.....	235
Editing rcigroup Attributes for User Members.....	235
Appendix C AC-DC Adapter and Rack Mount	239
AC-DC Adapter Clip Fitting	239
Identify the Clip Type.....	239
Remove the Attachment Cover from AC-DC Power Adapter.....	240
Attach the Clip to AC-DC Power Adapter	241
Bracket Installation.....	241
KX II-101 Bracket Parts	243
Attach the Brackets to KX II-101 for Horizontal Mount.....	243

Attach the Brackets to KX II-101 for Vertical Mount244

Appendix D Informational Notes **246**

Java Runtime Environment (JRE)246
Keyboard, Video and Mouse Notes246
 Sun Blade™ Video, Keyboard, and Mouse Support Limitation.....246
 Sun Keyboard Key Support Limitations.....247
 BIOS Access Limitation from a Local Keyboard.....247
 HP UX RX 1600 Keyboard and Mouse Configuration.....248
 Compaq Alpha and IBM P Server Mouse Mode Limitation248
 Windows 2000 and 2003 Server Keyboard Limitations.....249

Index **251**

Chapter 1 Introduction

In This Chapter

What's New in the User Guide	1
KX II-101 Overview.....	2
Product Photos	4
Product Features.....	5
Terminology.....	6
Package Contents	7
Optional Accessories.....	7
User Guide	7

What's New in the User Guide

The following sections of the user guide have changed or information has been added to based on enhancements and changes to the equipment and/or user documentation.

- Managing USB Connections (formerly managing target server settings). See **Managing USB Connections** (on page 165).
- Analog KVM Switch configuration. See **Analog KVM Switch** (on page 162).
- Pinout and supported operating system information has been added to the user guide. See **Specifications** (on page 222).

Please see the release notes for a more detailed explanation of the changes applied to this version of the user guide.

KX II-101 Overview

Thank you for purchasing the Dominion the KX II-101. The KX II-101 provides a single keyboard, video, and mouse (KVM) port for connection to a target server and a single IP port for connection to an IP network. Within the KX II-101 device, KVM signals from your server are converted to IP format and compressed for transmission over an IP network.

The KX II-101 dongle form-factor makes it easy to install near the target server, and each individual KX II-101 device has its own IP address. Each device is powered via Power-over-Ethernet (PoE) or an external AC-DC power pack.

The KX II-101 can operate as a standalone appliance or integrated into a single logical solution, along with other Raritan access products, using Raritan's CommandCenter Secure Gateway (CC-SG) management unit.

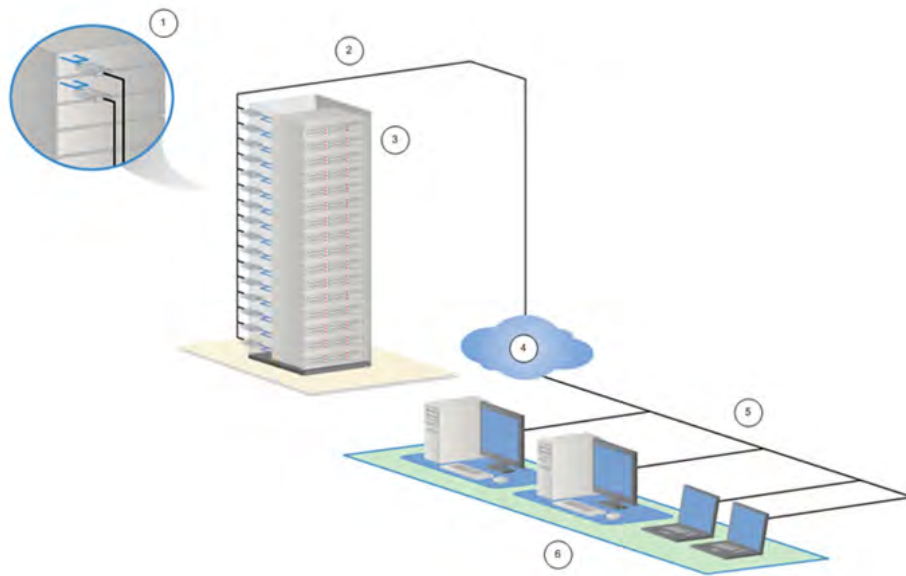











Diagram key	
	KX II-101
	LAN
	Windows, Linux, and Sun servers
	TCP/IP
	LAN
	Remote (network) access

Product Photos



Diagram key	
	KX II-101
	Mini-USB to USB cable
	Optional local port cable

Product Features

Interfaces

- Integrated PS/2 KVM connection
- USB connection for control and virtual media
- Serial Admin port for initial device configuration and diagnostics, as well as use with an external modem access and Raritan power strip control
- Ethernet LAN port supporting 10/100-base-T autosensing, full duplex
- LED network activity indicator and status
- Backlit LED power ON indicator

Network Configuration

- DHCP or static IP device address

System Management Features

- Firmware upgradable over Ethernet
- Failsafe firmware upgrade capability
- Clock that can be set manually or via synchronization with Network Time Protocol (NTP/SNTP)
- Local, timestamped, administrator activity log SNMP V2 agent that can be disabled by the administrator
- Support for RADIUS and LDAP/LDAPS authentication protocols

Administration Features

- Web-based management
- LDAP, Active Directory, RADIUS, or internal authentication and authorization
- DHCP or fixed IP addressing
- Integration with Raritan's CommandCenter Secure Gateway (CC-SG) management unit

User Features

- Web-based access through common browsers
- Intuitive graphical user interface (GUI)
- PC Share mode, which enables more than one remote user
- TCP communication
- English user interface
- Virtual media access
- Absolute Mouse Synchronization™
- Plug-and-play
- 256-bit encryption of complete KVM signal, including video and virtual media

Power

- Powered via Class 2 Power over Ethernet (PoE) provision
- Alternately powered by an external AC/DC power pack

Video Resolution

- Up to 1600X1200 at up to 60 Hz resolution

Mounting

- Rack mounting bracket

See **AC-DC Adapter and Rack Mount** (on page 239).

Terminology

Term	Description
Target Server	Server to be accessed remotely via the KX II-101 and its connected KVM configuration.
Remote PC	A Windows, Linux, or Apple Macintosh® computer used to access and control target servers connected to the KX II-101.
Admin serial port	Use the Admin serial port to connect to the serial port on the PC using the included Mini-DIN to DB9 cable. Then use a standard emulation software package (for example, HyperTerminal) to access the Admin serial port. The Admin serial port is used for network configuration.

Term	Description
Local User port	Enables a user in immediate proximity to the target server to use the native keyboard and mouse without unplugging the KX II-101.
Virtual media	Enables a KVM target server to remotely access media from client PC and network file servers.

Package Contents

Each KX II-101 device ships with:

- KX II-101 - KVM over IP
- USB Type A to Type B miniconnector
- Power Adaptor Kit - AC-DC 6VDC
- Three additional power outlet plugs for worldwide use
- Mini-DIN to DB9 serial cable
- Mounting bracket kit
- CD containing the Raritan User Guide & Quick Setup Guide
- Printed Quick Setup Guide
- Printed application release notes (if applicable)
- Printed technical notes (if applicable)

Optional Accessories

- DB15 to PS/2 and VGA Local User Cable

See **Connectors** (on page 226).

User Guide

The KX II-101 User Guide provides information on how to install, set up, and configure the KX II-101. It also includes information on accessing target servers and power strips, using virtual media, managing users and security, and maintaining and diagnosing the KX II-101.

Related Documentation

The KX II-101 User Guide is accompanied by a KX II-101 Quick Setup Guide, which can be found on the CD included with the device or on the Support page of Raritan's website (www.raritan.com). Installation requirements and instructions for client applications used with the KX II-101 can be found in the **KVM and Serial Client User Guide**, also found on the Raritan website. Where applicable, specific client functions used with the KX II-101 are included in this user guide.

Chapter 2 Installation and Configuration

In This Chapter

Overview9
Default Logon Information9
Getting Started10

Overview

This chapter describes how to install and configure the KX II-101. Installation and configuration consists of the following steps:

- **Step 1: Configure the Target Server** (on page 10)
- **Step 2: Configure Network Firewall Settings** (on page 16)
- **Step 3: Connect the KX II-101** (on page 17)
- **Step 4: Configure the KX II-101** (on page 24)

Before installing the KX II-101, in order to ensure optimum performance, first configure the target server you want to access via the KX II-101. Note that the following configuration requirements apply only to the target server, not to the computers that you will be using to access the KX II-101 remotely.

Default Logon Information

Default	Value
User name	The default user name is admin. This user has administrative privileges.
Password	The default password is raritan. 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 KX II-101, you are required to change the default password.
IP address	The KX II-101 ships with the default IP address of 192.168.0.192.

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

Getting Started

KX II-101 users with Microsoft Internet Explorer version 6 or Windows 2000 must upgrade to Service Pack 4 (SP4) or higher.

The KX II-101 ships with a static default IP address. On a network without a DHCP server, you must configure a new static IP address, net mask, and gateway address using either the KX II-101 serial admin console or the KX II-101 Remote Console.

See **Assigning an IP Address** (on page 25) for information on assigning an IP address to the KX II-101 using the Remote Console. See **Configure the KX II-101 Using a Terminal Emulation Program (Optional)** (on page 29) for information on setting an IP address using the Serial Admin Console.

Step 1: Configure the Target Server

Before installing the KX II-101, first configure the target server you want to access via the KX II-101 in order to ensure optimum performance. Note that the following configuration requirements apply only to the target server, not to the computers that you will be using to access the KX II-101 remotely.

Setting the Server Video Resolution

For optimal bandwidth efficiency and video performance, a target server running a graphical user interface such as Windows, X-Windows, Solaris, and KDE should be configured with desktop backgrounds set to a predominantly solid, light-colored graphic. Backgrounds featuring photos or complex gradients should be avoided.

Ensure that the server's video resolution and refresh rate are supported by the KX II-101 and that the signal is non-interlaced. The KX II-101 supports the following video resolutions:

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

Resolutions		
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

Sun™ Video Resolution

Sun systems have two resolution settings, a command line resolution and a GUI resolution. For information about the resolutions supported by the KX II-101, see **Setting the Server Video Resolution** (on page 10).

Note: If none of the supported resolutions work, make sure the monitor is multisync. Some monitors will not work with an H&V sync.

Command Line Resolution

► To check the command line resolution:

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

► To change the command line resolution:

1. Run the following command: `# eeprom output-device=screen:r1024x768x75` where `1024x768x75` is any resolution that the KX II-101 supports.
2. Restart the computer.

GUI Resolution/32 Bit

► To check the GUI resolution on 32 bit cards:

1. Run the following command: `# /usr/sbin/pgxconfig -prconf`

► To change the GUI resolution on 32 bit cards:

1. Run the following command: `# /usr/sbin/pgxconfig -res1024x768x75` where `1024x768x75` is any resolution that the KX II-101 supports.
2. Restart the computer.

GUI Resolution/64 Bit

▶ **To check the GUI resolution on 64 bit cards:**

1. Run the following command: `# /usr/sbin/m64config -prconf`

▶ **To change the resolution on 64 bit cards:**

1. Run the following command: `# /usr/sbin/m64config -res1024x768x75` where `1024x768x75` is any resolution that the KX II-101 supports.
2. Restart the computer.

GUI Resolution/Solaris 8

▶ **To check the resolution on Solaris 8 for 32 bit and 64 bit cards:**

1. Run the following command: `# /usr/sbin/fbconfig -prconf`

▶ **To change the resolution on Solaris 8 for 32 and 64 bit cards:**

1. Run the following command: `# /usr/sbin/fbconfig -res1024x768x75` where `1024x768x75` is any resolution that the KX II-101 supports.
2. Restart the computer.

Mouse Modes

The KX II-101 operates in several mouse modes: Absolute Mouse Synchronization™, Intelligent Mouse mode (do not use an animated mouse), and Standard Mouse mode.

Mouse parameters do not have to be altered for Absolute Mouse Synchronization. For both the Standard and Intelligent Mouse modes, mouse parameters must be set to specific values, which are described in this section.

Mouse configurations will vary on different target operating systems. Consult your OS documentation for additional details.

Windows 2000® Settings

▶ **To configure the mouse:**

1. Choose Start > Control Panel > Mouse.
2. On the Motion tab, set the acceleration to None and set the mouse motion speed setting to exactly the middle speed. Click OK.

▶ **To disable transition effects:**

1. Select the Display option from Control Panel.
2. On the Effects tab, deselect the Use the following transition effect for menus and tooltips checkbox. Click OK.

Windows XP®/Windows 2003® Settings**▶ To configure the mouse:**

1. Select Start > Control Panel > Mouse.
2. On the Pointer Options tab in the Motion group, set the mouse motion speed setting to exactly the middle speed and deselect the Enhanced pointer precision checkbox. Click OK.

▶ To disable transition effects:

1. Select Start > Control Panel > Display.
2. On the Appearance tab, click the Effects button.
3. Deselect the Use the following transition effect for menus and tooltips checkbox. Click OK.

Windows 2000 and XP Setting Notes

For a target server running Windows 2000 or XP, you may want to create a username to be used only for remote connections through the KX II-101. This allows you to keep the Target Server's slow mouse pointer motion/acceleration settings exclusive to the KX II-101 connection only, as other users may desire faster mouse speeds.

Windows 2000 or XP login screens revert to preset mouse parameters that differ from those suggested for optimal KX II-101 performance. Therefore, mouse sync will not be optimal at these screens. If you are comfortable adjusting the registry on Windows target servers, you can obtain better KX II-101 mouse synchronization at login screens by using the Windows registry editor to change the following settings:

- Default user mouse motion speed = 0; mouse threshold 1 = 0; mouse threshold 2 = 0.

Windows Vista® Settings**▶ To configure the mouse:**

1. Select Start > Settings > Control Panel > Mouse.
2. On the Pointer Options tab in the Motion group, set the mouse motion speed setting to exactly the middle speed and deselect the Enhanced pointer precision option. Click OK.

▶ To disable animation and fade effects:

1. Select Start > Settings > Control Panel > System > Advanced system settings. The System Properties dialog appears.
2. Click the Advanced tab and click the Settings button in the Performance group. The Performance Options dialog appears.
3. Under Custom options, deselect the following checkboxes:

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

Linux® Settings

On a target server running Linux graphical interfaces, set the mouse acceleration to exactly 1 and set threshold to exactly 1. Enter the command `xset mouse 1 1`.

Ensure that a target server running Linux is using a resolution supported by the KX II-101 at a standard VESA resolution and refresh rate. A Linux target server should also be set so the blanking times are within +/- 40% of VESA standard values.

► **To check for these parameters:**

1. Go to the Xfree86 Configuration file XF86Config.
2. Using a text editor, disable all non-KX II-101 supported resolutions.
3. Disable the virtual desktop feature, which is not supported by the KX II-101.
4. Check blanking times (+/- 40% of VESA standard).
5. Restart the computer.

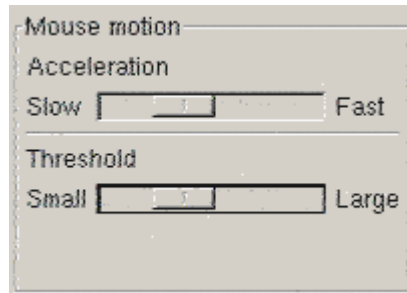
Note: In many Linux graphical environments, the command `Ctrl+Alt+ +` (plus sign) changes the video resolution, scrolling through all available resolutions that remain enabled in the XF86Config file.

Sun® Solaris™ Settings

A Solaris target server must be configured to one of the display resolutions supported by the KX II-101. The most popular supported resolutions for Sun machines are:

Resolution
1024x768@60Hz
1024x768@70Hz
1024x768@75Hz
1024x768@85Hz
1280x1024@60Hz

Set the mouse acceleration value to exactly 1 and the threshold to exactly 1. A target server running the Solaris operating system must output VGA video (H-and-V sync, not composite sync). Set this at the graphical user interface or with the command line `xset mouse a t` where `a` is the acceleration and `t` is the threshold.



► **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 `#eeprom output-device=screen:r1024x768x75` command to change the output resolution.
3. Issue the boot command to reboot the server.

Alternatively, contact your Raritan representative to purchase a video output adapter. Suns with composite sync output require APSSUN II Raritan guardian for use with the KX II-101. HD15 Suns with separate sync output require an APKMSUN Raritan guardian for use with the KX II-101.

Apple Macintosh® Settings

Mac works with the KX II-101 'out of the box.' However, you must use Absolute Mouse Synchronization and enable Absolute Mouse mode and mouse scaling for Mac servers on the KX II-101 Port page.

► **To enable this setting:**

1. Choose Device Settings > Port Configuration. The Port Configuration Page opens.
2. Click the Port Name for the port you want to edit.
3. In the USB Connection Settings section, select the Enable Absolute Mouse checkbox and the "Enable Absolute mouse scaling for MAC server" checkbox. Click OK.

See **Port Configuration** (on page 154).

IBM AIX® Settings

1. Go to the Style Manager.

2. Click on Mouse Settings and set the Mouse Acceleration to 1.0 and Threshold to 3.0.

Step 2: Configure Network Firewall Settings









To access the KX II-101 through a network firewall, your firewall must allow communication on TCP Port 5000. Alternatively, the KX II-101 can be configured to use a different TCP port of your own designation.

To take advantage of the KX II-101's web-access capabilities, the firewall must allow inbound communication on TCP Port 443 - the standard TCP port for HTTPS communication. To take advantage of the KX II-101's redirection of HTTP requests to HTTPS (so that users may type the more common, `http://xxx.xxx.xxx.xxx`, instead of `https://xxx.xxx.xxx.xxx`), the firewall must also allow inbound communication on TCP Port 80 - the standard TCP port for HTTP communication.

Step 3: Connect the KX II-101

The KX II-101 has the physical connections described in the diagram.



Diagram key		
	Admin port	Use to do one of the following: <ul style="list-style-type: none"> • Configure and manage the device with a terminal emulation program on your PC. • Configure and manage a power strip. • Connect an external modem to dial into the device.
	Monitor and PS/2 cable	Attached Monitor and PS/2 cable (see E).
	Mini-USB port	Use to connect the device to the target server with the included USB cable if not using the attached PS/2 cable. A USB connection must be used to utilize the Absolute Mouse Synchronization or virtual media features.
	Power indicator	Backlit LED power ON and boot-up indicator. Provides feedback on the operating status of the device.
	Monitor and PS/2 cable	Attached Monitor and PS/2 cable. Use to connect the device to a monitor and to a target server if not using the USB cable.
	Power connector	Connects the power supply if you are not using a PoE (Power over Ethernet) LAN connection.
	Local user port	Use to connect a local keyboard, video, and mouse directly to the target server using an optional PS/2 cable.
	Ethernet LAN/PoE port	Provides LAN connectivity and power if using a PoE LAN connection.

Power

The KX II-101 can be powered with either the included standard AC power pack or by PoE (Power over Ethernet).

- For standard AC power, plug the included AC power adaptor kit into the Power port and plug the other end into a nearby AC power outlet.
- For PoE, attach a 10/100Mbps cable to the LAN port and plug the other end into a PoE-provisioned LAN.

After the KX II-101 is powered ON, it goes through a boot-up sequence, during which the blue Raritan-logo LED will blink for about 45 seconds. Upon successful boot-up, the back-lit LED remains lit.

Target Server

The KX II-101 can use either the included USB cable or integrated PS/2 cables to connect to the target server. Before connecting, configure your target server's video to a supported resolution.

Note: For PS/2 configurations that require virtual media connectivity, the USB connector is also necessary.

USB Configuration

► **To configure the KX II-101 for use with a USB target server:**



1. Connect the mini-USB connector to the KX II-101 and the USB connector to a USB port on the target server.
2. Use the attached video cable to connect the KX II-101 to the target video port.
3. Use the optional PS/2 DKX2-101-LPKVMC cabling to attach only the local video to the Local User port of the KX II-101. **Optional**

Note: The KX II-101 must be powered for the Local User port to function.

Use USB cables to connect the keyboard and mouse directly to the target server.



Diagram key	
A	Target server
B	Included mini-USB to USB cable from the KX II-101 to the target server
C	KX II-101
D	Local monitor, keyboard, and mouse
1	USB connection from the target server to mouse

Diagram key	
	USB connection from the target server to keyboard
	Video connection to the local monitor (optional cable)

PS/2 Configuration

► **To configure the KX II-101 for use with a PS/2 target server:**

1. Use the attached PS/2 keyboard, video, and mouse cabling to connect the KX II-101 to the target server.
2. Use the PS/2 cabling to attach the local keyboard, video, and mouse to the Local User port of the KX II-101.

Note: The KX II-101 must be powered for the Local User port to function.

- If you require Virtual Media (VM) connectivity, connect the mini-USB connector to the KX II-101 and the USB connector to any USB port on the target server.

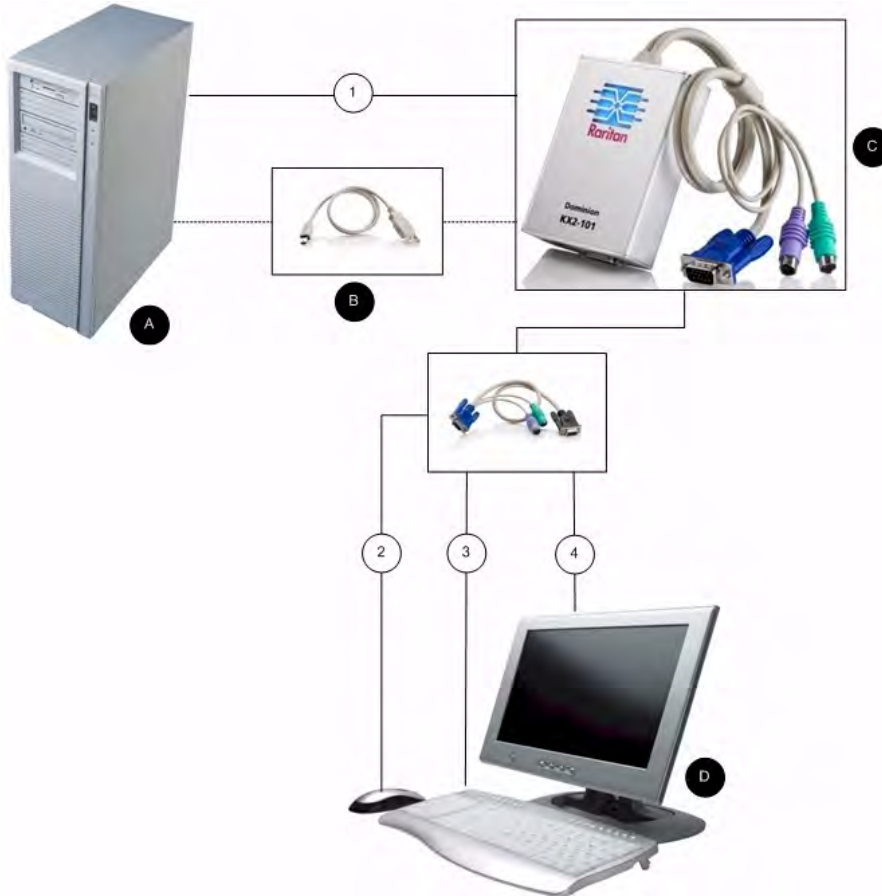





Diagram key

A	Target server
B	Included mini-USB to USB connector from the KX II-101 to the target server for Virtual Media connectivity
C	KX II-101
D	Local monitor, keyboard, and mouse
1	Integrated PS/2 keyboard, video, and mouse connections from the KX II-101 to the target server

Diagram key	
	PS/2 connection from the KX II-101 to the mouse (optional cable)
	PS/2 connection from the KX II-101 to the keyboard (optional cable)
	Video connection to the local monitor (optional cable)

Network

Connect a standard Ethernet cable from the network port labeled LAN to an Ethernet switch, hub, or router. The LAN LEDs that appear above the Ethernet connection indicate Ethernet activity. The yellow one blinks while the KX II-101 is in use, indicating IP traffic at 10 Mbps. The green light indicates a 100 Mbps connection speed.

Admin Port

The Admin port enables you to perform configuration and setup for the KX II-101 using a terminal emulation program like HyperTerminal. Plug the min-DIN end of the included serial cable into the Admin port of the KX II-101 and plug the DB9 end into a serial port on your PC or laptop. The serial port communication settings should be configured to the following:

- 115,200 Baud
- 8 data bits
- 1 stop bit
- No parity
- No flow control

See ***Configure the KX II-101 Using a Terminal Emulation Program (Optional)*** (on page 29) for additional information on using a terminal emulation program.

Local User Port

The KX II-101 is available with optional video and PS/2 cables (KX II-101-LPKVMC) that enable you to attach a keyboard and mouse to the target server through the Local User port. The Local User port serves as a pass-through to the target server to which the KX II-101 is attached and has no other purpose. The KX II-101 must be powered on to use the Local User port.

For USB configurations, only the local video connects to the target server at the Local User port. The keyboard and mouse connect directly to the target server using USB ports.

Note: Only PS/2 host interface connectivity is supported on the Local User port and you must restart the target server after connecting to the KX II-101 using PS/2 connectors.

Step 4: Configure the KX II-101

The KX II-101 can be configured in two ways:

- Using the web-based KX II-101 Remote Console, which requires the device to have a network connection to your workstation.
- Using a terminal emulation program like HyperTerminal, which requires a direct connection from the device's Admin port to your workstation. The cable for this connection is included with the KX II-101.

This section describes both ways of configuring the KX II-101.

Configure the KX II-101 Using the Remote Console

The KX II-101 Remote Console is a web-based application that enables you to configure the device prior to use and manage it after it has been configured. Before configuring the KX II-101 using the Remote Console, you must have both your workstation and the device connected to a network.

You can also use a terminal emulation program to configure the KX II-101. See **Configure the KX II-101 Using a Terminal Emulation Program (Optional)** (on page 29).

Setting a New Password

When you first log into the Remote Console, you are prompted to set a new password to replace the default. Then you can configure the KX II-101.

1. Log into a workstation with network connectivity to your KX II-101 device.

2. Launch a supported web browser such as Internet Explorer (IE) or Firefox.
3. In the address field of the browser, enter the default IP address of the device: 192.168.0.192.
4. Press Enter. The login page opens.
5. Enter the user name admin and the password raritan.
6. Click Login. The Change Password page is displayed.
7. Type raritan in the Old Password field.
8. Type a new password in the New Password field and the Confirm New Password field. Passwords can be up to 64 characters long and can consist of English alphanumeric and printable special characters.
9. Click Apply. You will receive confirmation that the password was successfully changed.
10. Click OK. The Port Access page opens.

Assigning an IP Address

1. In the KX II-101 Remote Console, choose Device Settings > Network. The Network Settings page opens.
2. In the Device Name field, specify a meaningful name for your KX II-101 device. You can enter up to 16 alphanumeric and special characters with no spaces.
3. Select the IP configuration from the IP auto configuration drop-down list:
 - None (Static IP) - This is the default and recommended option because the KX II-101 is an infrastructure device and its IP address should not change. This option requires that you manually specify the network parameters.

- DHCP - With this option, network parameters are assigned by the DHCP server each time the KX II-101 is booted.

Home > Device Settings > Network Settings

Network Basic Settings

Device Name ^{*}
DavidCDKX2-101

IP Address

IP Address 192.168.59.169	Subnet Mask 255.255.255.0
Default Gateway 192.168.59.126	Preferred DHCP Host Name

IP Auto Configuration
None

Obtain DNS Server Address Automatically

Use the Following DNS Server Addresses

Primary DNS Server IP Address

Secondary DNS Server IP Address

OK Reset To Defaults Cancel

Configuring Direct Port Access

► **To configure direct port access:**

1. Choose Device Settings > Device Services. The Device Services page opens.
2. Select the Enable Direct Port Access via URL checkbox.
3. Enable global TELNET or SSH access.
 - Select the Enable TELNET Access checkbox to enable TELNET access.
 - Select the Enable SSH Access checkbox to enable SSH access.

4. Specify a valid TCP port for the selected access type. For example, direct port access via Telnet TCP port can be configured as 7770.
5. Click OK.

See **Device Management** (on page 138) for more information.

Home > Device Settings > Device Services

Services

Discovery Port *
5000

Enable TELNET Access

TELNET Port
23

Enable SSH Access

SSH Port
22

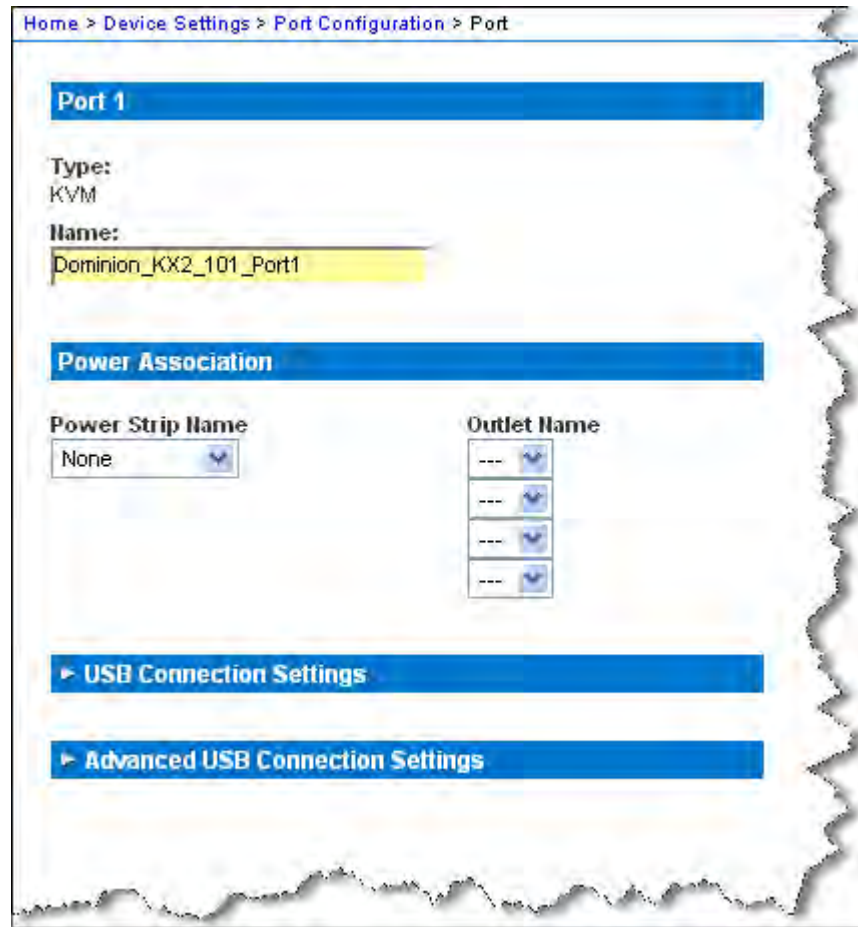
Enable Direct Port Access via URL

OK Reset To Defaults Cancel

Naming the Target Server

1. Attach the KX II-101 to the target server.
2. Choose Device Settings > Port Configuration. The Port Configuration page opens.
3. Click the Port Name for the target server. The Port page opens.
4. Type a name, up to 32 alphanumeric and special characters.

5. Click OK.



Remote Authentication

Note to CC-SG Users

When the KX II-101 is controlled by CommandCenter Secure Gateway, CC-SG authenticates users and groups.

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

Supported Protocols

To simplify management of usernames and passwords, the KX II-101 provides the ability to forward authentication requests to an external authentication server. Two external authentication protocols are supported: LDAP/LDAPS and RADIUS.

Note on Microsoft Active Directory

Microsoft Active Directory uses the LDAP/LDAPS protocol natively, and can function as an LDAP/LDAPS server and authentication source for the KX II-101. If it has the IAS (Internet Authorization Server) component, a Microsoft Active Directory server can also serve as a RADIUS authentication source.

Create User Groups and Users

As part of the initial configuration, you must define user groups and users in order for users to access the KX II-101.

The KX II-101 uses system-supplied default user groups and allows you to create groups and specify the appropriate permissions to suit your needs.

User names and passwords are required to gain access to the KX II-101. This information is used to authenticate users attempting to access your KX II-101.

See **User Management** (on page 116) for details on adding and editing user groups and users.

Configure the KX II-101 Using a Terminal Emulation Program (Optional)

You can use the Admin serial console with a terminal emulation program like HyperTerminal to set the following configuration parameters for the KX II-101:

- IP address
- Subnet mask address
- Gateway address
- IP access control
- LAN speed
- LAN interface mode

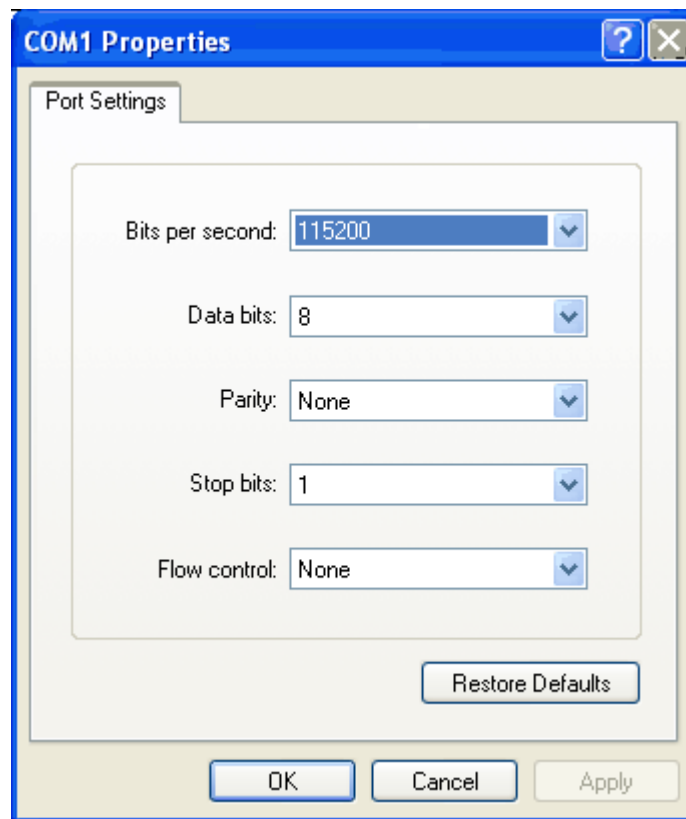
To use a terminal emulation program with the KX II-101, you must first connect the included RS-232 serial cable from the Admin port on the KX II-101 to the COM1 port on your PC. See **Admin Port** (on page 23).

For demonstration purposes, the terminal emulation program described in this section is HyperTerminal. You can use any terminal emulation program.

► To use a terminal emulation program to configure the KX II-101:

1. Connect the KX II-101 to a local PC using the included RS-232 serial cable.
2. Connect to the Admin port on the KX II-101 and the COM1 port on the PC.

3. Launch the terminal emulation program you want to use to configure the KX II-101.
4. Set the following port settings in the terminal emulation program:
 - Bits per second - 115200
 - Data bits - 8
 - Parity - None
 - Stop bits - 1
 - Flow control - None



5. Connect to the KX II-101. The login page opens.
6. Type the administrator user name and press Enter. You are prompted to enter your password.
7. Type your password and press Enter. The Admin Port prompt appears.
8. At the Admin Port > prompt, type *config* and press Enter.
9. At the Config > prompt, type *network* and press Enter.
10. To view the current interface settings, at the Interface > prompt, type *interface* and press Enter. The current interface settings appear.

11. To configure new network settings, at the Network prompt, type *interface* followed by one of the following commands and its appropriate argument (option), then press Enter.

Command	Argument	Options
ipauto	none dhcp	<p>none - Enables you to manually specify an IP address for the device. You must follow this option with the ip command and the IP address, as shown in the following example:</p> <pre>interface ipauto none ip 192.168.50.12</pre> <p>dhcp - Automatically assign an IP address to the device on startup.</p>
ip	IP address	The IP address to assign to the device. To manually set an IP address for the first time, this command must be used with the ipauto command and the none option. See ipauto for information. After you have manually assigned an IP address once, you can use the ip command alone to change the IP address.
mask	subnetmask	The subnet mask IP address.
gw	IP address	The gateway IP address
mode	mode	<p>The Ethernet mode. You have the following choices:</p> <ul style="list-style-type: none"> ▪ auto - Automatically sets speed and interface mode based on the network. ▪ 10hdx - 10 MB/s, half duplex. ▪ 10fdx - 10 MB/s, full duplex ▪ 100hdx - 100 MB/s, half duplex ▪ 100fdx - 100 MB/s, full duplex

- When you have successfully changed a setting, you see a confirmation message like the following:

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

1. When you are finished configuring the KX II-101, type *logout* at the command prompt and press Enter.

You are logged out of the command line interface.

Chapter 3 Working with Target Servers

In This Chapter

Interfaces	32
Virtual KVM Client	41
Multi-Platform Client (MPC).....	60

Interfaces

KX II-101 Remote Console Interface

The KX II-101 Remote Console is a browser-based graphical user interface that allows you to log into KVM target servers and serial targets connected to the KX II-101 and to remotely administer the KX II-101.

The KX II-101 Remote Console provides a digital connection to your connected KVM target servers. When you log into a KVM target server using the KX II-101 Remote Console, a Virtual KVM Client window opens.

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

1. In IE7, click Tools > Internet Options to open the Internet Options dialog.
 2. In the "Temporary Internet files" section, click the Settings button. The Settings dialog opens.
 3. In the "Check for newer versions of stored pages" section, select Automatically.
 4. Click OK to apply the settings.
-

Enable Direct Port Access

Direct port access enables you to access the KX II-101 Remote Client without having to go through the usual login page. With direct port access enabled, you can define an URL to navigate directly to the Port Access page.

► **To enable direct port access:**

1. Launch the KX II-101 Remote Console.
2. Choose Device Settings > Device Services. The Device Services page opens.
3. Select the Enable Direct Port Access via URL checkbox.

4. Click Save.

► **To define a direct port access URL:**

- Define a URL with the IP address, user name, password, and if necessary, port number of the KX II-101.

If you have only one KVM port, the port number is not needed.

The format for a direct port access URL is:

```
https://IP
address/dpa.asp?username=username&password=password&port=
port number
```

Tip: Define a direct port access URL once, then save it in your web browser as a bookmark to make reusing it easier.

KX II-101 Remote Console Interface

The KX II-101 Remote Console is a browser-based graphical user interface that allows you to log into KVM target servers and serial targets connected to the KX II-101 and to remotely administer the KX II-101.

The KX II-101 Remote Console provides a digital connection to your connected KVM target servers. When you log into a KVM target server using the KX II-101 Remote Console, a Virtual KVM Client window opens.

KX II-101 Console Navigation

The KX II-101 Console interfaces provide many methods for navigation and making your selections.

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

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

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

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

Port Access Page

After successfully logging in to the KX II-101 Remote Console, the Port Access page appears. This page lists the KX II-101 port, the connected KVM target server, and its status and availability. The Port Access page provides access to the KVM target server connected to the KX II-101. A KVM target server is a server that you want to control through the KX II-101 device. They are connected to the KX II-101 ports at the back of the device.

► To use the Port Access page:

1. From the KX II-101 Remote Console, click the Port Access tab. The Port Access page opens.

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

- Port Number - The port available for the KX II-101 device.
 - Port Name - The name of the KX II-101 port. Initially, this is set to `Dominion_KX2_101_Port1` but you can change the name to something more descriptive. When you click a Port Name link, the Port Action Menu appears.
 - Status - The status is either up or down.
 - Availability - The Availability can be Idle, Connected, Busy, or Unavailable.
2. Click the Port Name of the target server you want to access. The Port Action Menu appears. See **Port Action Menu** (on page 34) for details on available menu options.
 3. Choose the desired menu command from the Port Action Menu.

Port Action Menu

When you click a Port Name in the Port Access list, the Port Action menu appears. Choose the desired menu option for that port to execute it. Note that only options available for the selected port are listed in the Port Action menu:

- Connect - Creates a new connection to the target server. For the KX II-101 Remote Console, a new **Virtual KVM Client** (on page 41) page appears.

Note: This option is not available from the KX II-101 Remote Console for an available port if all connections are busy.

- Disconnect - Disconnects this port and closes the Virtual KVM Client page for this target server. This menu item is available only when the port status is up and connected, or up and busy.
- Power On - Powers on the target server through the associated outlet. This option is visible only when there are one or more power associations to the target.
- Power Off - Powers off the target server through the associated outlets. This option is visible only when there are one or more power associations to the target, when the target power is on (port status is up), and when user has permission to operate this service.
- Power Cycle - Power cycles the target server through the associated outlets. This option is visible only when there are one or more power associations to the target, and when the user has permission to operate this service.

Managing Favorites

A Favorites feature is provided so you can organize and quickly access the devices you use frequently. The Favorite Devices section is located in the lower left side (sidebar) of the Port Access page and provides the ability to:

- Create and manage a list of favorite devices
- Quickly access frequently-used devices
- List your favorites either by Device Name, IP Address, or DNS hostname
- Discover KX II-101 devices on its subnet (before and after login)
- Retrieve discovered KX II-101 devices from the connected KX device (after login)

► **To access a favorite KX II-101 device:**

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

► **To display favorites by name:**

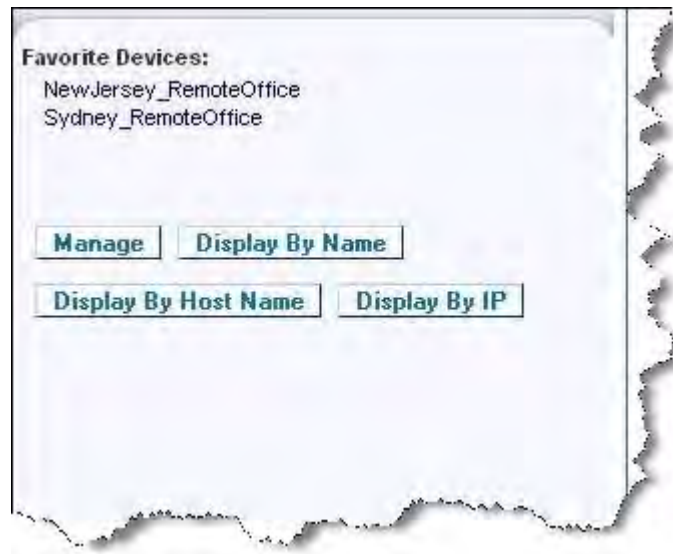
- Click Display by Name.

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

- Click Display by IP.

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

- Click Display by Host Name.



Manage Favorites Page▶ **To open the Manage Favorites page:**

- Click the Manage button in the left panel. The Manage Favorites page appears and contains the following:

Use:	To:
Favorites List	Manage your list of favorite devices.
Discover Devices - Local Subnet	Discover Raritan devices on the client PC's local subnet.
Discover Devices - KX II-101 Subnet	Discover the Raritan devices on the KX II-101 device subnet.
Add New Device to Favorites	Add, edit, and delete devices from your list of Favorites.

Favorites List Page

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.

Discovering Raritan Devices on the Local Subnet

This option discovers the devices on your local subnet, which is the subnet where the KX II-101 Remote Console is running. These devices can be accessed directly from this page or you can add them to your list of favorites. See **Favorites List Page** (on page 37).

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

1. Choose Manage > Discover Devices - Local Subnet. The Discover Devices - Local Subnet page appears.
2. Choose the appropriate discovery port:
 - To use the default discovery port, select the Use Default Port 5000 checkbox.
 - To use a different discovery port:
 - a. Deselect the Use Default Port 5000 checkbox.
 - b. Type the port number in the Discover on Port field.
 - c. Click Save.

3. Click Refresh. The list of devices on the local subnet is refreshed.

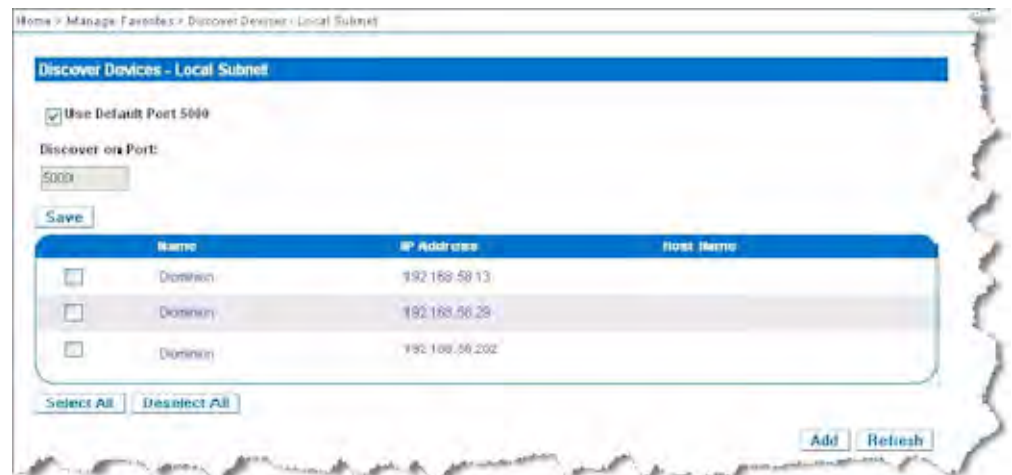
► **To add devices to your Favorites List:**

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

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:**

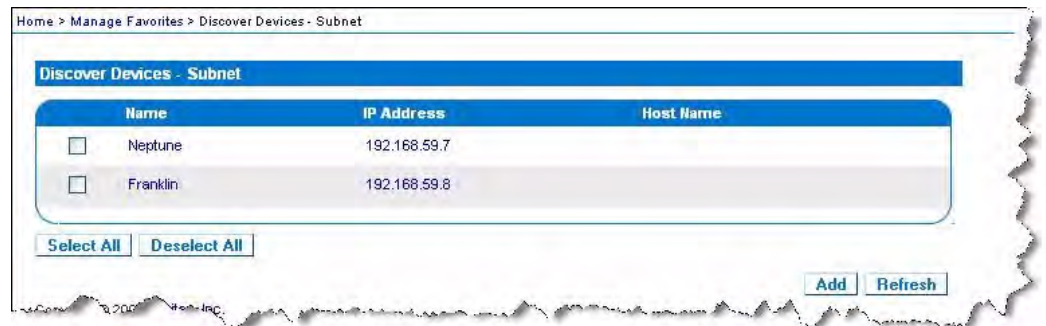
- Click the device name or IP address for that device. A new browser opens to that device.



Discovering Raritan Devices on the KX II-101 Subnet

This option discovers devices on the device subnet, which is the subnet of the KX II-101 device IP address itself. You can access these devices directly from this the Subnet page or add them to your list of favorites. See **Favorites List Page** (on page 37).

This feature allows multiple KX II-101 devices to interoperate and scale automatically. The KX II-101 Remote Console automatically discovers the KX II-101 devices, and any other Raritan device, in the subnet of the KX II-101.



► To discover devices on the device subnet:

1. Choose Manage > Discover Devices - KX II-101 Subnet. The Discover Devices - KX II-101 Subnet page appears.
2. Click Refresh. The list of devices on the local subnet is refreshed.

► To add devices to your Favorites List:

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

Tip: Use the Select All and Deselect All buttons to quickly select all (or deselect all) devices in the KX II-101 device subnet.

► To access a discovered device:

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

Adding, Deleting, and Editing Favorites

► To add a device to your favorites list:

1. Choose Manage > Add New Device to Favorites. The Add New Favorite page appears.
2. Type a meaningful description.
3. Type the IP Address/Host Name for the device.

4. Change the discovery Port (if necessary).
5. Select the Product Type.
6. Click OK. The device is added to your list of favorites.

Home > Manage Favorites > Add New Favorite

Add New Favorite

All fields are required

Description

IP Address/Host Name

Port

Product Type

▼

► **To edit a favorite:**

1. From the Favorites List page, select the checkbox next to the appropriate KX II-101 device.
2. Click the Edit button. The Edit page appears.
3. Update the fields as necessary:
 - Description
 - IP Address/Host Name - Type the IP address of the KX II-101 device
 - Port (if necessary)
 - Product Type
4. Click OK.

► **To delete a favorite:**

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

1. Select the checkbox next to the appropriate KX II-101 device.
2. Click the Delete button. The favorite is removed from your list of favorites.

Logging off

► **To quit the KX II-101 Remote Console:**

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

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

Multi-Platform Client Interface

See **Multi-Platform Client (MPC)** (on page 60).

Virtual KVM Client

Overview

Whenever you access a target server using the KX II-101 Remote Console, a Virtual KVM Client (VKC) window opens. There is one Virtual KVM Client for each target server connected. These windows can be accessed via the Windows task bar.

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 exercise caution.

Connecting to a KVM Target Server

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

1. From the KX II-101 Remote Console, click the Port Access tab to open it. The Port Access page opens.
2. Click the Port Name of the target you want to access. The Port Action menu appears.
3. Click Connect. A **Virtual KVM Client** (on page 41) window opens to the target server connected to that port.

VKC Toolbar

Button	Description
	Properties
	Video settings
	Calibrate color
	Synchronize the target mouse cursor
	Refresh screen
	Auto-sense video
	Send Ctrl+Alt+Delete
	Single mouse cursor
	Full screen
	Resize video to fit screen

Power Controlling a KVM Target Server

*Note: These features are available only when you have made power associations. See **Power Control** (on page 157).*

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

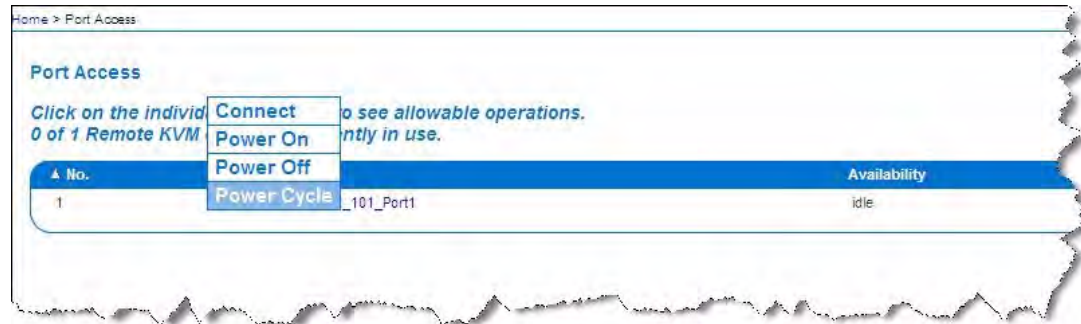
1. From the KX II-101 Remote Console, click the Port Access tab. The Port Access page opens.
2. Click the Port Name of the appropriate target server. The Port Action menu appears.
3. Choose Power Cycle. A confirmation message appears.

► **To power on a target server:**

1. From the KX II-101 Remote Console, click the Port Access tab. The Port Access page opens.
2. Click the port name of the appropriate target server. The Port Action menu appears.
3. Choose Power On. A confirmation message appears.

► **To power off a target server:**

1. From the KX II-101 Remote Console, click the Port Access tab to open it. The Port Access page opens.
2. Click the port name of the appropriate target server. The Port Action menu appears.
3. Choose Power Off. A confirmation message appears.



Disconnecting a KVM Target Server

► **To disconnect a target server:**

1. Click the port name of the target you want to disconnect. The Port Action menu appears.
2. Choose Disconnect.


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

VKC Connection Properties

The KX II-101 dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. The KX II-101 devices optimize KVM output not only for LAN use, but also for WAN use. These devices can also control color depth and limit video output, offering an optimal balance between video quality and system responsiveness for any bandwidth.

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

► **To set the connection properties:**

1. Choose Connection > Properties or click the Connection Properties button  in the toolbar. The Properties dialog appears.

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

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

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

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

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

Connection Information

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

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

The following information is displayed about the current connection:

- Device Name - The name of the KX II-101 device.
- IP Address - The IP address of the KX II-101 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 Options

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.

Building a Keyboard Macro

► **To build a macro:**

1. Click Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.
2. Click Add. The Add Keyboard Macro dialog then appears.
3. Type a name for the macro in the Keyboard Macro Name field. This name will appear in the Keyboard menu after it is created.
4. From the Hot-Key Combination field, select a keyboard combination from the drop-down list. This allows you to execute the macro with a predefined keystroke. **Optional**
5. In the Keys to Press drop-down list:
 - a. Select each key you would like to use to emulate keystrokes. Select the keys in the order by which they are to be pressed.
 - b. After each selection, select Press Key. As each key is selected, it will appear in the Keys to Release field.

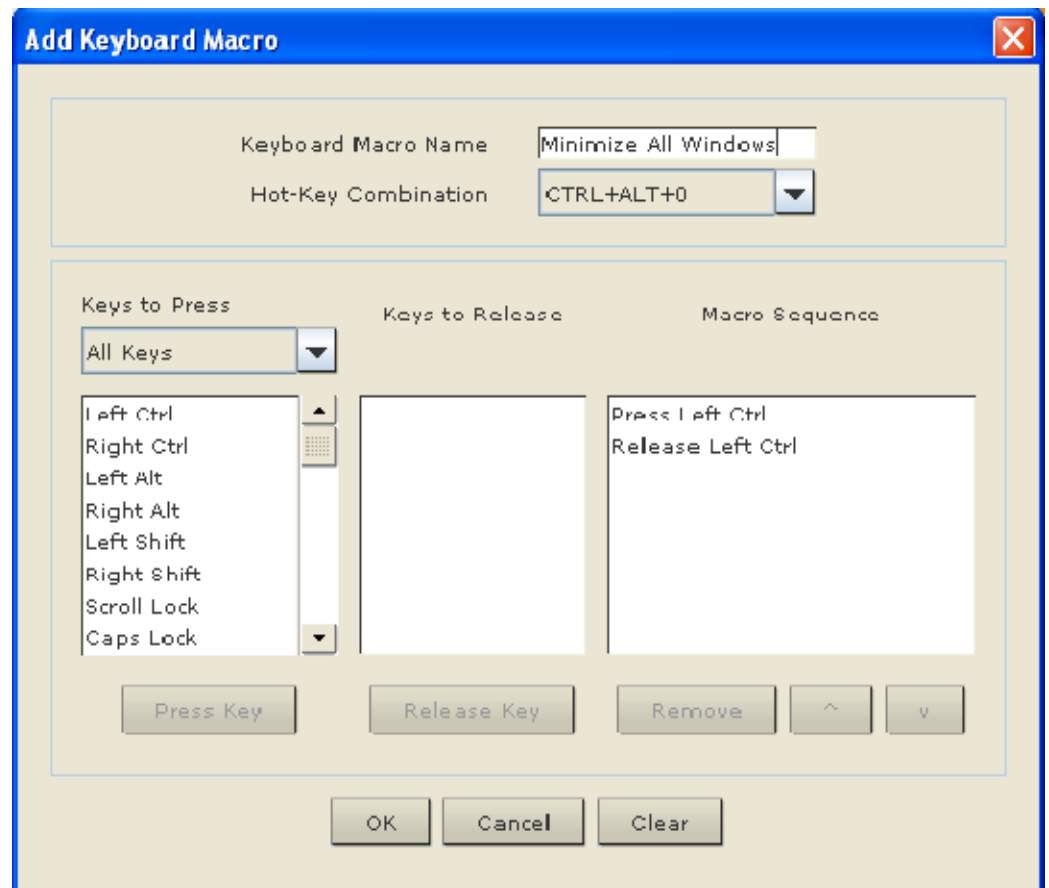
For example, select the Windows key and the letter D key. When these keys are selected in the client, the macro will be executed. Add a key release attribute to the macro if needed (see next step).
6. In the Keys to Release field:
 - a. Choose each key for which you would like to emulate a key release. Define the keys you want released in order to run the macro.

For example, specify that the keys to be pressed must also be released in order for the macro to be executed. Select the keys in the order by which they are to be released.
 - b. Click Release Key after each selection.

7. Review the Macro Sequence field to be sure the macro sequence is defined correctly.

The contents of this field are automatically generated and are based on the selections made in the Keys to Press and Keys to Release fields.

- a. To remove a step in the sequence, select it and click Remove.
 - b. To change the order of steps in the sequence, click the step and then click the up or down arrow buttons to reorder them as needed.
8. Click OK to save the macro. Click Clear to clear all field and start over. When you click OK, the Keyboard Macros dialog appears and lists the new keyboard macro.



9. Click Close to close the Keyboard Macros dialog. The macro will now appear on the Keyboard menu in the application. Select the new macro on the menu to run it or use the keystrokes you assigned to the macro.



Running a Keyboard Macro

Once you have created a keyboard macro, execute it using the keyboard macro you assigned to it or by choosing it from the Keyboard menu.

Run a Macro from the Menu Bar

When you create a macro, it appears under the Keyboard menu. Execute the keyboard macro by clicking on it in the Keyboard menu.

Run a Macro Using a Keyboard Combination

If you assigned a keyboard combination to a macro when building it, you can execute the macro by pressing its assigned keystrokes. For example, press the keys Ctrl+Alt+0 simultaneously to minimize all windows on a Windows target server.

Modifying and Removing Keyboard Macros

► To modify a macro:

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

5. Click OK.

► **To remove a macro:**

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

Video Properties


Refresh Screen

The Refresh Screen command forces a refresh of the video screen. Video settings can be refreshed automatically in several ways:

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

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


► **To refresh the video settings, do one of the following:**

- Choose Video > Refresh Screen or click the Refresh Screen button  from toolbar.

Auto-Sense Video Settings

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

► **To automatically detect the video settings, do the following:**


- Choose Video > Auto-sense Video Settings or click the Auto-Sense Video Settings button  in the toolbar. A message stating that the auto adjustment is in progress appears.

Calibrate Color

Use the Calibrate Color command to optimize the color levels (hue, brightness, saturation) of the transmitted video images. The KX II-101 color settings are on a target server-basis.

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


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

- Choose Video > Calibrate Color or click the Calibrate Color button  in the toolbar. The target device screen updates its color calibration.

VKC Video Settings

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

► **To change the video settings:**

1. Choose Video > Video Settings or click the Video Settings button  in the toolbar to open the Video Settings dialog.
2. Adjust the following settings as required. As you adjust the settings the effects are immediately visible:

- a. Noise Filter

The KX II-101 device 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.

- b. Brightness: Use this setting to adjust the brightness of the target server display.
- c. Brightness Red - Controls the brightness of the target server display for the red signal.
- d. Brightness Green - Controls the brightness of the green signal.
- e. Brightness Blue - Controls the brightness of the blue signal.
- f. Contrast Red - Controls the red signal contrast.
- g. Contrast Green - Controls the green signal.
- h. Contrast Blue - Controls the blue signal.

If the video image looks extremely blurry or unfocused, the settings for clock and phase can be adjusted until a better image appears on the active target server.

Warning: Exercise caution when changing the Clock and Phase settings. Doing so may result in lost or distorted video and you may not be able to return to the previous state. Contact Raritan Technical Support before making any changes.

- i. Clock - Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended. Under most circumstances this setting should not be changed because the autodetect is usually quite accurate.
 - j. 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.
 - k. Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor.
3. Vertical Offset - Controls the vertical positioning of the target server display on your monitor.
 4. Select the video sensing mode:
 - Best possible video mode
The KX II-101 device will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.
 - Quick sense video mode
With this option, the KX II-101 device will use a quick video Auto Sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.
 5. Click OK to apply the settings and close the dialog. Click Apply to apply the settings without closing the dialog.

Note: Some Sun background screens, such as screens with very dark borders, may not center precisely on certain Sun servers. Use a different background or place a lighter colored icon in the upper left corner of the screen.



Mouse Options

When controlling a target server, the KX II-101 Remote Console displays two mouse cursors: one belonging to your client workstation and the other belonging to the target server.

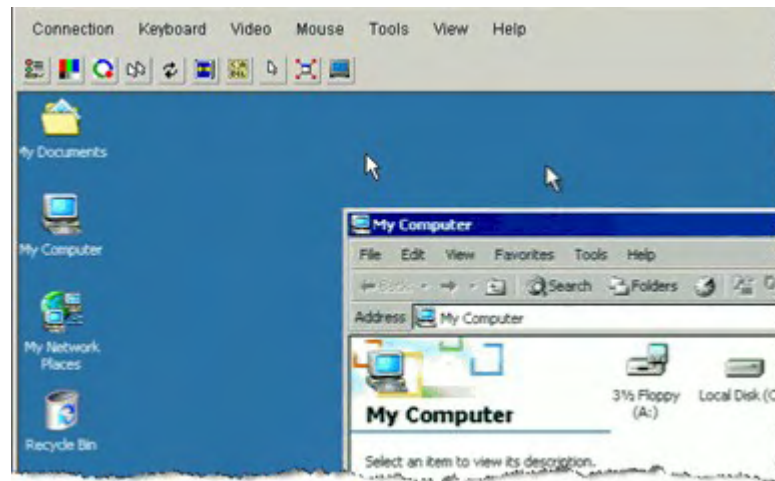
You can operate in either single mouse mode or dual mouse mode. When in dual mouse mode, and provided the option is properly configured, the mouse cursors will align.

When there are two mouse cursors, the KX II-101 device offers several mouse modes:

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

Mouse Pointer Synchronization

When remotely viewing a target server that uses a mouse, you will see two mouse cursors: 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).

Mouse Synchronization Tips

Be sure to follow these steps when configuring mouse synchronization:

1. Verify that the selected video resolution and refresh rate are among those supported by the KX II-101 device. The Virtual KVM Client Connection Info dialog displays the actual values that the KX II-101 is seeing.
2. Verify that the cable length is within the specified limits for the selected video resolution.
3. Verify that the mouse and video have been properly configured during the installation process.
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.

Synchronize Mouse

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

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

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

Standard Mouse Mode

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

▶ **To enter standard mouse mode:**

- Choose Mouse > Standard.

Absolute Mouse Mode

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

▶ **To enter absolute mouse mode:**

- Choose Mouse > Absolute.

Note: The absolute mouse setting requires a USB target system and is the recommended mouse setting for KX II-101.

Intelligent Mouse Mode

In Intelligent Mouse mode, the KX II-101 device can detect the target mouse settings and synchronize the mouse cursors 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.

► **To enter intelligent mouse mode:**

- Choose Mouse > Intelligent.

Intelligent Mouse Synchronization Conditions

The Intelligent Mouse Synchronization command, available on the Mouse menu, automatically synchronizes mouse cursors during moments of inactivity. For this to work properly, however, the following conditions must be met:

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- Advanced mouse properties such as “Enhanced pointer precision” or “Snap mouse to default button in dialogs” should be disabled.
- Choose “Best Possible Video Mode” in the Video Settings window.
- The edges of the target video should be clearly visible (that is, a black border should be visible between the target desktop and the remote KVM console window when you scroll to an edge of the target video image).
- When using the intelligent mouse synchronization function, having a file icon or folder icon located in the upper left corner of your desktop may cause the function not to work properly. To be sure to avoid any problems with this function, Raritan recommends you do not have file icons or folder icons in the upper left corner of your desktop.

After autosensing the target video, manually initiate mouse synchronization by clicking the Synchronize Mouse button on the toolbar. This also applies when the resolution of the target changes if the mouse cursors start to desync from each other.


If intelligent mouse synchronization fails, this mode will revert to standard mouse synchronization behavior.

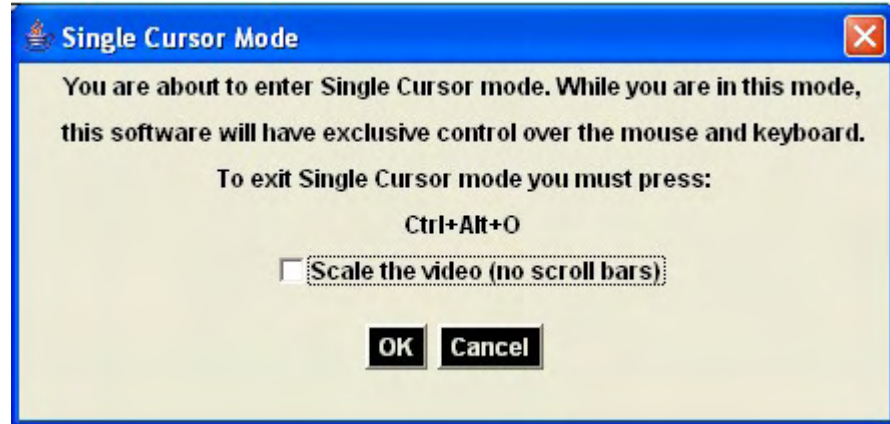
Please note that mouse configurations will vary on different target operating systems. Consult your OS guidelines for further details. Also note that intelligent mouse synchronization does not work with UNIX targets.

Single Mouse Cursor

Single Mouse mode uses only the target server mouse cursor and the local mouse pointer no longer appears onscreen. While in single mouse mode, the Synchronize Mouse command is not available (there is no need to synchronize a single mouse cursor).

► **To enter single mouse mode, do the following:**

1. Choose Mouse > Single Mouse Cursor.
2. Click the Single/Double Mouse Cursor button  in the toolbar.



► **To exit single mouse mode:**

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

VKC Virtual Media

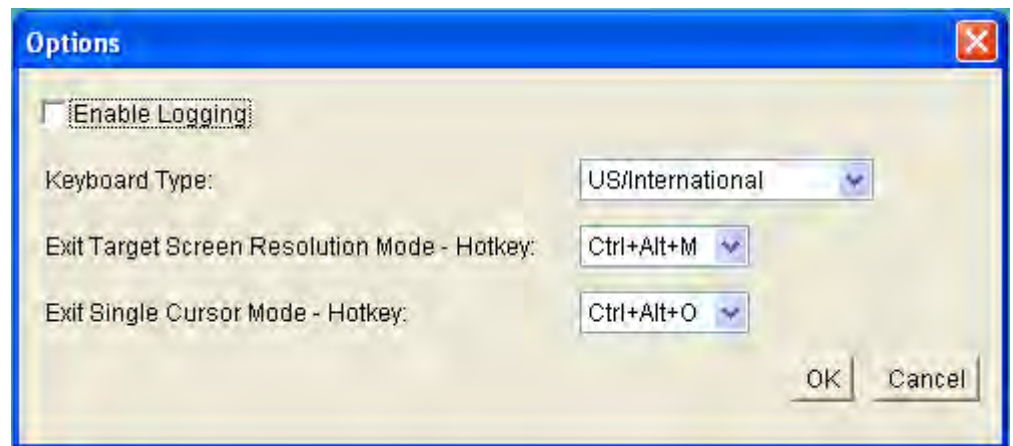
See the chapter on *Virtual Media* (on page 106) for complete information about setting up and using virtual media.

Tool Options

From the Tools menu, you can specify certain options for use with the Virtual KVM Client, including logging, setting the keyboard type, and defining hot keys for exiting target screen resolution mode and single cursor mode.

► **To set the tools options:**

1. Choose Tools > Options. The Options dialog appears.



2. Select the Enable Logging checkbox only if directed to by Technical Support. This option creates a log file in your home directory.
3. Choose the Keyboard Type from the drop-down list (if necessary). The options include:
 - US/International
 - French (France)
 - German (Germany)
 - Japanese
 - United Kingdom
 - Korean (Korea)
 - Belgian (Belgium)
 - Norwegian (Norway)
 - Danish (Denmark)
 - Swedish (Sweden)
 - German (Switzerland)
 - Hungarian (Hungary)
 - Spanish (Spain)

- Italian (Italy)
 - Slovenian
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 hot key used for exiting this mode.
 5. Exit Single Cursor Mode - Hotkey. When you enter single cursor mode, only the target server mouse cursor is visible. This is the hot key used to exit single cursor mode and bring back the client mouse cursor.
 6. Click OK.

Keyboard Limitations

Slovenian Keyboards

The < key does not work on Slovenian keyboards due to a JRE limitation.

Language Configuration on Linux

Because the Sun JRE on Linux has problems generating the correct Key Events for foreign-language keyboards configured using System Preferences, Raritan recommends that you configure foreign keyboards using the methods described in the following table.

Language	Configuration method
US Intl	Default
French	Keyboard Indicator
German	System Settings (Control Center)
Japanese	System Settings (Control Center)
UK	System Settings (Control Center)
Korean	System Settings (Control Center)
Belgian	Keyboard Indicator
Norwegian	Keyboard Indicator
Danish	Keyboard Indicator
Swedish	Keyboard Indicator
Hungarian	System Settings (Control Center)
Spanish	System Settings (Control Center)
Italian	System Settings (Control Center)
Slovenian	System Settings (Control Center)

Note: The Keyboard Indicator should be used on Linux systems using Gnome as a desktop environment.

View Options

View Toolbar

You can use the Virtual KVM client with or without the toolbar display.

▶ **To toggle the display of the toolbar (on and off):**

- Choose View > View Toolbar.

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.

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 hot key used for exiting this mode is specified in the Options dialog (the default is Ctrl+Alt+M).

▶ **To enter target screen resolution:**

- Choose View > Target Screen Resolution.

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

Press the hot key configured in the Tools Options dialog. The default is Ctrl+Alt+M.

Help Options

About Raritan Virtual KVM Client

This menu command provides version information about the Virtual KVM Client, in case you require assistance from Raritan Technical Support.

▶ **To obtain version information:**

- Choose Help > About Raritan Virtual KVM Client.

Multi-Platform Client (MPC)

Raritan Multi-Platform Client (MPC) is a graphical user interface for the Raritan product lines, providing remote access to target servers connected to Raritan KVM over IP devices.

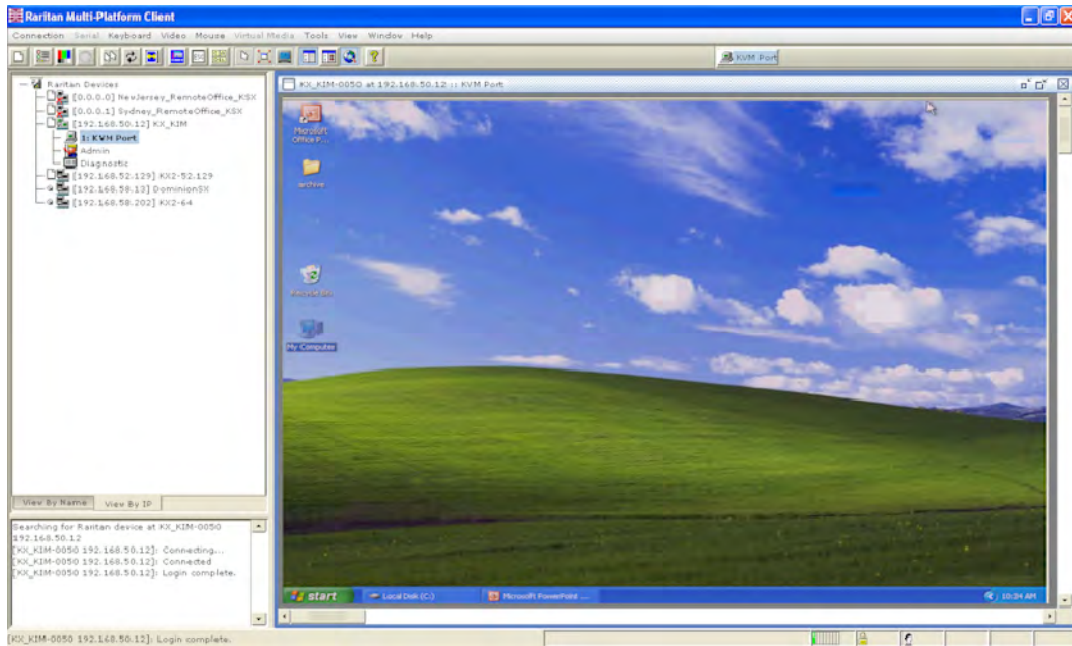
Requirements and Installation

If you do not have MPC installed, for information on MPC installation requirements and directions on how to install MPC, see the **KVM and Serial Client User Guide**. This guide can be accessed on the **Raritan website** <http://www.raritan.com> on the Support page.

Operation

MPC Interface

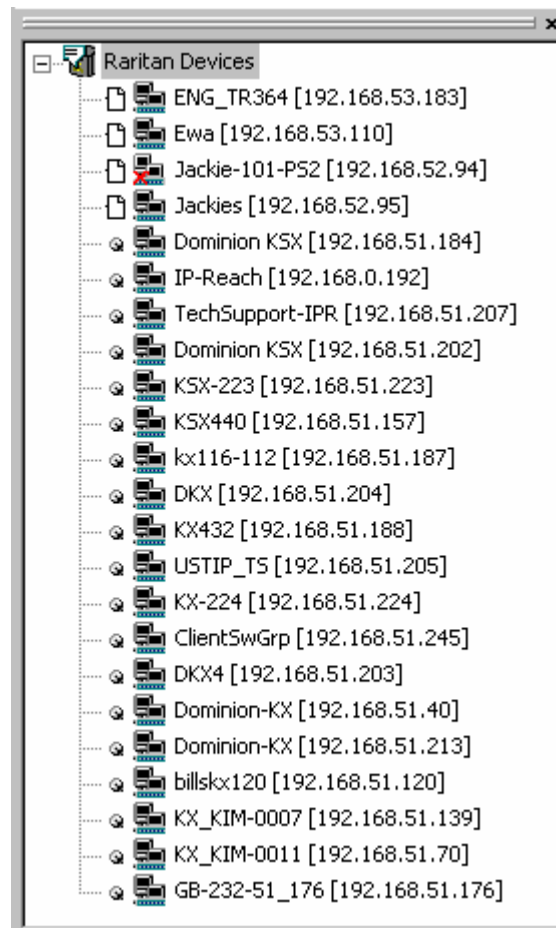
MPC functions are grouped into six general sections on the page. As a standalone product or using a web browser, the MPC window contains these main sections.



Navigator

The navigator provides a tree view of every known Raritan device. From this panel, you can access all Raritan networked devices for which a connection profile exists and/or all Raritan devices automatically identified on the network.

Note: Automatic Raritan device identification uses the UDP protocol and will typically identify all Raritan devices on your subnet. Network administrators rarely allow UDP broadcasts to function outside of a subnet. Automatic Raritan device identification will find only those Raritan devices that are configured to use the default TCP Port (5000) or another broadcast port, which is defined on the Advanced tab of the Options dialog (choose Tools > Options to access the Options dialog).



Devices in the MPC Navigator

In MPC, devices are named according to the Manager Name field on the Manager's Network Configuration page. Dominion devices are named according to the Device Name field on the Dominion Console Network Settings page.

Device Ports in the Navigator

For each device to which you are connected, you are able to expand the tree associated with it to see each device port to which you have access. Ports with a green icon indicate that you are connected to that port. The port that is bolded in the Navigator indicates that it is the port currently displayed (active) in the remote desktop area of the application.




If no name is assigned to a port, by default it is listed in the Navigator as 'Unnamed' for Generation 1 devices and, for the KX II, as Dominion_KX2_PortN (N = port number).

Depending on the maximum number of KVM sessions the device can handle at once, if all device ports to which you are connecting are already occupied, an alert message appears and you must wait until one of the ports is available in order to connect.




Navigator Icons

Each device in the Navigator is assigned two icons. One icon represents the device's connection profile and the other icon represents its network status. A connection profile is generally created by a user in order to store personalized information about specific devices (see **Connection Profiles** (on page 74) for additional information). The connection status indicates the current status of the device.

Device Connection Profile Icons (Left Icon)





Icon	Description
	Profiled - A network connection profile exists for this device.
	Modem Profile - A modem connection profile exists for this device.
	Not Profiled - The device was found on the network but a connection profile does not exist for it.

Device Network Status Icons (Right Icon)

Icon	Description
	Connected (green) - You are currently authenticated and connected to this device.
	Available (black) - This device is currently available on the network but you are not currently connected to it.
	Unavailable - A profile exists for this device but it is not currently available on the network. (Note that all devices to which you <i>are not</i> currently connected and that have modem profiles will use this icon.)




Port Connection Status Icons

For each server port listed in the Navigator, the following icons can be associated with it depending on its status:

Icon	Description
	Connected
	Available for connection.
	Unavailable (either no device is connected or access is blocked).
	In use by another user (may be unavailable depending on permissions).

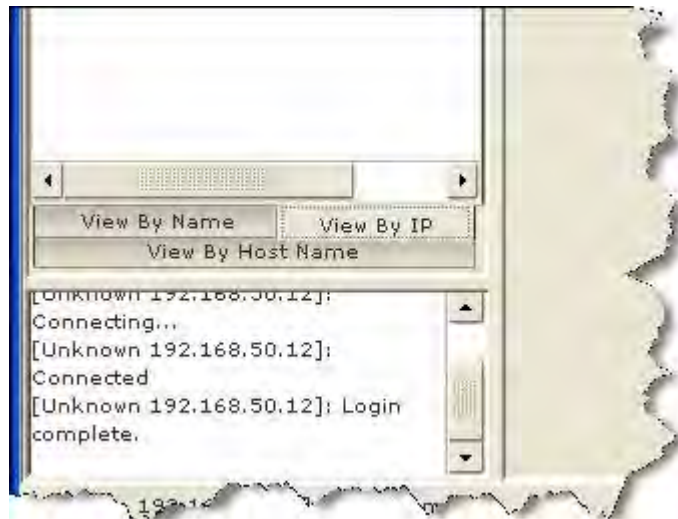
Customizing the Navigator

Use specific tools in the toolbar to customize some Navigator attributes:

Icon	Action	Description
	Display/Hide Navigator	You can also select Navigator in the View menu to toggle between displaying and hiding the Navigator.
	Refresh Navigator	Updates the device status information displayed in the Navigator.
	Browse Discovered Devices	When enabled, Show Discovered Devices will display devices that are “not profiled” but have been found on the network. This option can also be enabled by choosing View > Show > Discovered Devices. <i>Note: The Browse Discovered Devices option is the only method of connecting to a Raritan device configured to use a DHCP IP address.</i>

MPC Navigator Tabs

MPC tabs at the base of its Navigator pane. These tabs allow you to change how you display devices. Click the View By Name tab to sort the list alphabetically by name, click the View By IP tab to sort the list numerically by IP address, or click on the View by Host Name tab to sort the list alphabetically by display name.

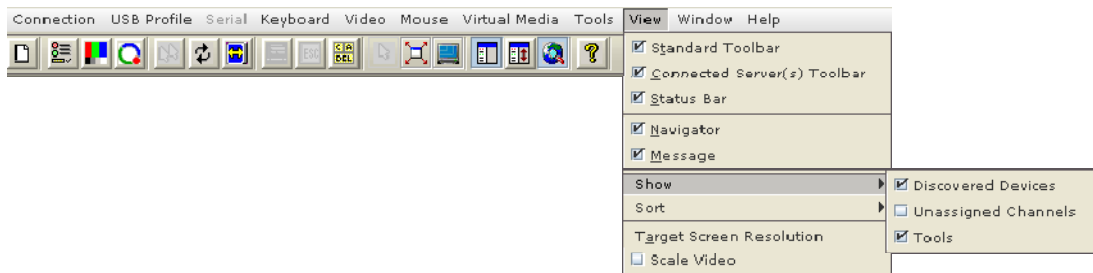


These tabs are available only in the MPC interface.

Navigator Display Options

Showing Ports

- Discovered Devices - Shows or hides discovered devices from the Navigator view. You will not see broadcast messages when this option is disabled (not selected).
- Unassigned Channels - Shows or hides channels with no assigned targets. Note that the default for Generation 1 (G1) devices is to show unassigned channels (option is enabled), whereas the default is to hide unassigned channels (option is disabled) for Generation 2 (G2) devices.
- Tools - Shows or hides the Admin and Diagnostic ports.



Note: These settings are saved from session to session.

Toolbars


Standard Toolbar








The Standard toolbar provides one-click access to the most frequently-used commands.








► To display the Standard toolbar:



- Choose View > Standard Toolbar.

Following is a list of the buttons in the standard toolbar as well as a description of the action performed once the buttons are selected. Additionally, if there are menu options or shortcut menu options that will perform the same task, they are listed, too.

Button	Button Name	Description
	New Profile	Creates a new Navigator entry for a Raritan device. Same result as choosing Connection > New Profile in the menu.

Button	Button Name	Description
	Connection Properties	<p>Opens the Modify Connection Properties dialog from which you can manually adjust bandwidth options (such as connection speed, color depth, and so forth).</p> <p>Same as choosing Connection > Properties or choosing Connection Properties on the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.</p>
	Video Settings	<p>Opens the Video Settings dialog, allowing you to manually adjust video conversion parameters.</p> <p>Same as choosing Video > Video Settings or choosing Video Settings on the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.</p>
	Color Calibration	<p>Adjusts color settings to reduce excess color noise.</p> <p>Same as choosing Video > Color Calibrate.</p>
	Synchronize Mouse	<p>In dual-mouse mode, forces realignment of the target server mouse pointer with the mouse pointer.</p> <p>Same as choosing Mouse > Synchronize Mouse or choosing Synchronize Mouse on the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.</p>
	Refresh Screen	<p>Forces a refresh of the video screen.</p> <p>Same as choosing Video > Refresh Screen or choosing Refresh Screen on the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.</p>
	Auto-sense Video Settings	<p>Forces a refresh of the video settings (resolution, refresh rate).</p> <p>Same as choosing Video > Auto-sense Video Settings.</p>
	Enter On-Screen Menu	<p>Not applicable for the device. Used by the application with other Raritan products.</p> <p>Same as choosing Keyboard > Enter On-Screen Menu.</p>

Button	Button Name	Description
	Exit On-Screen Menu	<p>Not applicable for IP-Reach or Dominion. Used by the application with other Raritan products.</p> <p>Alternatively, select Esc on the keyboard. Same as choosing Keyboard > Exit On-Screen Menu.</p> <hr/> <p><i>Note: This function is not available on the KSX II.</i></p>
	Send Ctrl+Alt+Del	<p>Sends a Ctrl+Alt+Del hot key combination to the target server.</p> <p>Same as choosing Keyboard > Send Ctrl+Alt+Del.</p>
	Single Cursor Mode	<p>Starts Single Cursor mode in which the local mouse pointer no longer appears onscreen.</p> <p>Same as choosing Mouse > Single Cursor Mode. Press Ctrl+Alt+X to exit this mode. Alternatively, choose Single/Double Cursor from the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.</p>
	Full Screen Mode	<p>Maximizes the screen real estate to view the target server desktop.</p> <p>Same as choosing View > Target Screen Resolution (in MPC) or Full Screen (in RRC). Alternatively, press Ctrl+Left Alt+M to open the shortcut menu and then choose Full/Normal Screen or press the F key on your keyboard.</p>
	Scaling	<p>Increases or reduces the target video size so you can view the entire contents of the target server window without using the scroll bar.</p>
	Show/Hide Navigator	<p>Toggles the Navigator panel between visible and hidden.</p> <p>Same as choosing View > Navigator.</p>
	Refresh Navigator	<p>Forces a refresh of the data displayed in the Navigator.</p>

Button	Button Name	Description
	Show/Hide Browse All Devices	Toggles between displaying and not displaying Raritan devices in the Navigator that are automatically identified on the network and that do not have preconfigured profiles associated with them.
	About	Displays the application version information. Same as choosing Help in the menu bar.

MPC Connected Server(s) Toolbar

The Connected Server(s) toolbar is comprised of a button for each connected target server port, thus enabling quick access to connected targets. When you connect to a port, a button corresponding to that port is added to the toolbar and labeled with the name of the port. Conversely, when you disconnect from a port, the corresponding button is removed from the toolbar.

Note: In Single Mouse mode, the Connected Server(s) Toolbar appears on the target but cannot be accessed.

By default, the Connected Server(s) toolbar is enabled (visible). To disable it, deselect Connected Server(s) Toolbar in the View menu. Buttons corresponding to windows that do not support full screen mode are not shown in the toolbar. For example, serial ports, generation one (G1) admin ports, and G1 diagnostic ports will not be displayed in the toolbar in full screen mode.

While in full screen mode, you are able to view the Connected Server(s) toolbar by hovering your mouse over the top of the screen. To use this feature, the Connected Servers Toolbar option must be selected in the View menu.



► **To display the Connected Server(s) toolbar (when not already visible):**

- Choose View > Connected Server(s) Toolbar.

► **To view the window for a target server:**

- Click the button that corresponds to the appropriate connected target server you want to view. The window for the corresponding target server is displayed and the button for the selected port is highlighted. In full screen mode, note that this action is window swapping, not video switching.

When you click a button that is already highlighted, the corresponding window is minimized. If you click that button again, the window is brought forward and maximized.

MPC Status Bar

The status bar displays session information about your connection to a Raritan device. This information includes:

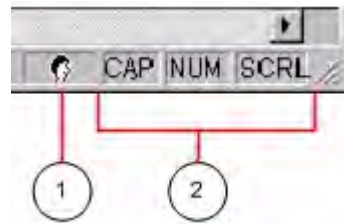



Diagram key	Session information	Description
①	Concurrent connections indicator	<p>Indicates that multiple remote users are currently connected to the same target server on the device.</p> <p>One icon indicates a single user is connected, and two icons indicates two or more users are connected.</p> <p>Concurrent connection ability can be set globally under PC share mode on the Manager Security Settings page or set per individual user in the Concurrent Access Mode setting on the Manager User Account Settings page. For the KX II-101 device, concurrent connection ability can be set using the PC Share Mode option in the Security Settings page: PC-Share permits concurrent access and Private limits server access to one user at a time.</p>

Diagram key	Session information	Description
	Lock key indicators	Indicates the status of the current target KVM Server, in respect to the activation of the Caps-Lock, Num-Lock, and Scroll-Lock keys. If these keys are enabled on the target server being viewed, this affirmative status will be reflected on the status bar.

Note: If a light is used on your keyboard to indicate the Scroll Lock, Num Lock, and Caps Lock key is active, it may or may not be in sync with the lock key indicator status displayed on the status bar. See the status bar as your guide if this occurs.


Screen Modes

Besides a standard view, full screen view and a scaling option are available. These options increase the remote desktop area and make viewing the target video easier.

MPC Target Screen Resolution Mode

Target Screen Resolution mode provides you with the ability to view the target server desktop in full screen mode, which removes all toolbars from view.

Activate Target Screen Resolution mode once you are connected to a target by doing one of the following:

- Click the Full Screen button  in the toolbar and then click OK in the confirmation message that appears.
- Choose View > Target Screen Resolution and then click OK in the confirmation message that appears.
- Press Ctrl+Left Alt+M to open the shortcut menu. Next, press the F key on your keyboard or use your mouse to choose Full/Normal Screen. Click OK in the confirmation message that appears.



To exit full screen mode, use the shortcut menu or click the Close icon



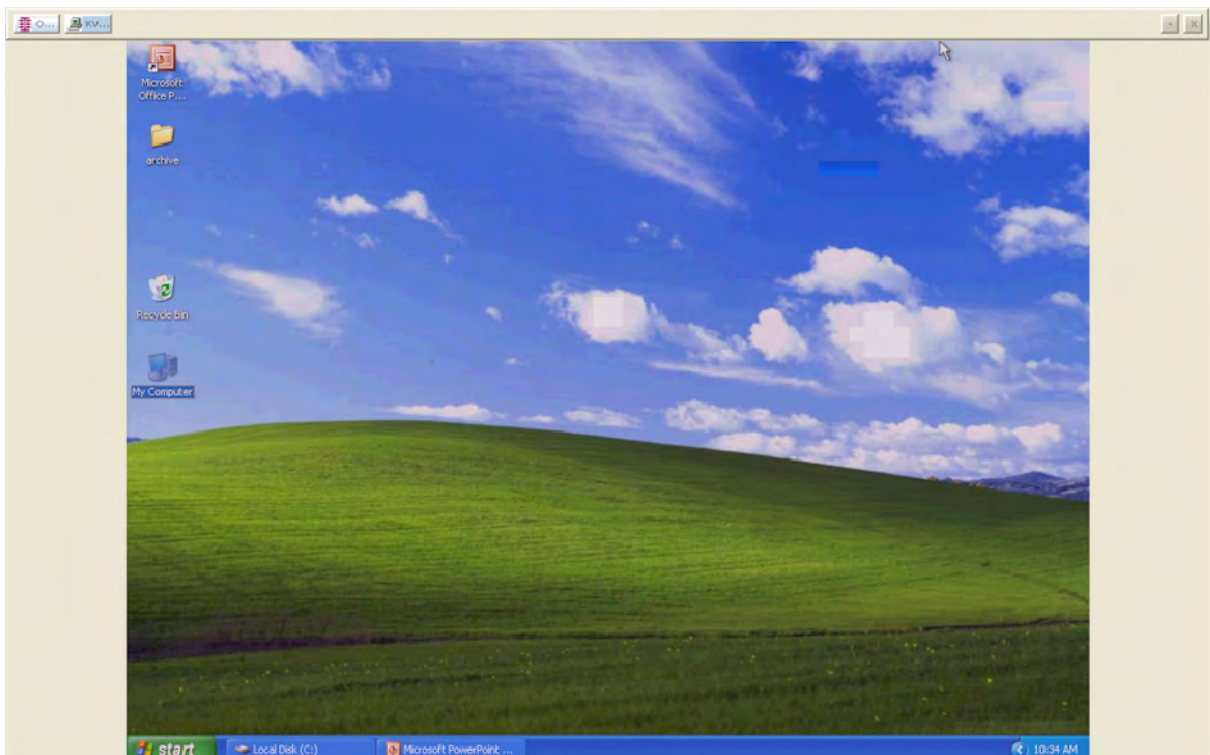
that appears at the top right of the page when you hover your mouse along the top of the screen.

Note: The Ctrl+Left Alt+M key combination does not work for certain target servers if you are running JRE 1.5.0_01. To return from full page mode, use Alt+Tab and choose MPC.

While in full screen mode, you are able to view the Connect Server toolbar by hovering your mouse over the top of the screen. To use this feature, the Connected Servers Toolbar option must be selected in the View menu.

Additionally, while in full screen mode, your monitor's resolution may be adjusted to match the resolution of the target server (provided your graphics system supports it). If your graphics system does not support the resolution of the target system, you will be unable to activate full screen mode and a message will appear requesting that you change your video resolutions first.

Tip: To view the video resolutions your system supports in a Windows environment, access your computer's Control Panel from the Windows Start menu, double-click Display, and click the Settings tab.

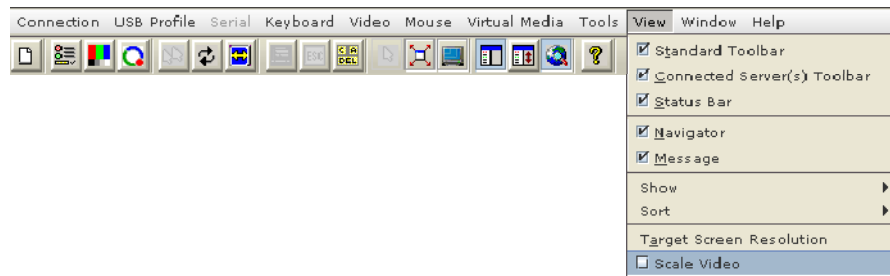



MPC Scaling

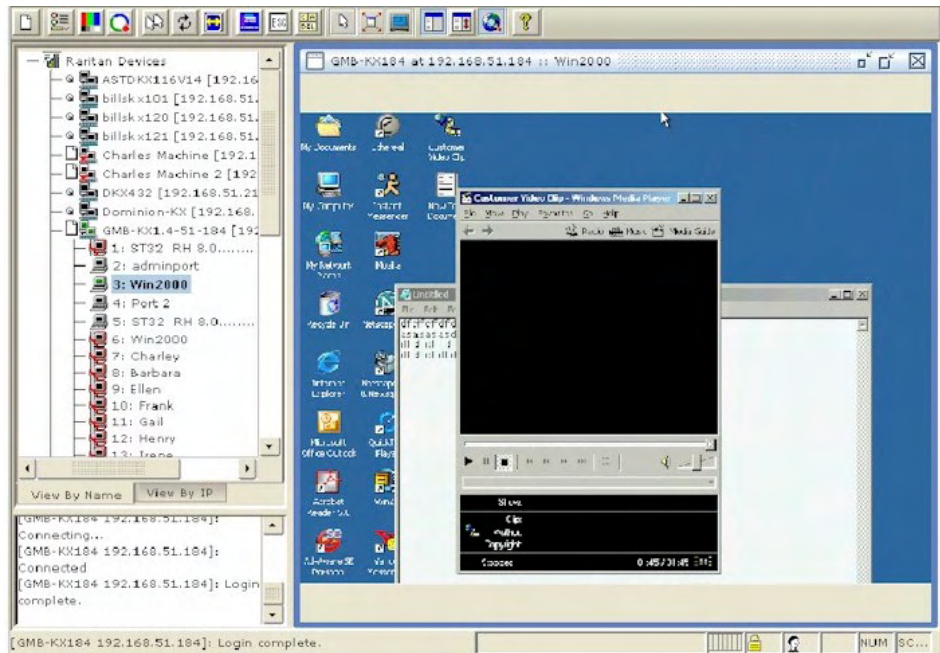
Scaling your target window size allows you to view the entire contents of the target server window. This feature increases or reduces the size of the target video to fit the window size and maintains the aspect ratio. This allows you to see the entire target server desktop while in standard view.

► **To activate Scaling, do one of the following:**

- Choose View > Scale Video.



- Click the Scaling button  on the toolbar.
- To exit this mode and return the target window to its previous size, deselect Scale Video on the View menu or click the Scaling button once again.



Note: Enabling Scale Video will scale the complete target video image to fit the remote desktop area as it grows or shrinks. You can combine this setting with target screen resolution for a full page affect on targets with a higher resolution than your desktop.

Auto-Scroll

The auto-scroll feature automatically scrolls the video display in the direction of the cursor as the cursor approaches the edge of the display. A thin border appears around the perimeter of the remote desktop area to indicate the function is on. When enabled, if you see scroll bars and then move the cursor onto the border, the page will automatically scroll in the appropriate direction.

The scroll border is activated by selecting Show Scroll Borders in the Options dialog, which is accessed by choosing Tools > Options.

Connection Profiles

Connection profiles store important information about your Raritan device such as the IP address, custom TCP ports, preferred compression settings, and custom security keys. A profile is required to access devices outside your subnet and to access devices using a dial-up connection.

Through profiles, you can set up personalized connections. These profiles are not shared among other users.

The information collected when creating a new connection profile will differ based on Generation 1 and Generation 2 devices.

Tip: If your Raritan device is configured to use a custom TCP port or a group security key, first create a connection profile so that you can access the device.

Creating, Modifying and Deleting Profiles in MPC

► To create a profile:

1. There are two ways to create a profile:
 - For automatically discovered devices, right-click the device name in the Navigator and choose Add Profile from the shortcut menu.
 - For other devices, choose Connection > New Profile.

The Add Connection dialog appears. Options are organized into three tabs.

Note: The Connection and Security tabs are not available for Generation 2 devices.

2. On the Connect tab, type a meaningful description of the device in the Description field (up to 32 alphanumeric and special characters are allowed). This description identifies the Raritan device in the Navigator.
3. From the Product drop-down, choose the Raritan product you are using.
4. Select the type of connection from the Connection Type drop-down.

TCP/IP connections

- a. If TCP/IP Connection is selected for a LAN/WAN connection, complete the information in the "Find Raritan device By" section:
 - Type the IP address assigned to your Raritan device.
 - Type the name assigned to your Raritan device during initial setup.
 - Type the Domain Name Server (DNS) name. Use this option if you use a DNS server to resolve a DNS name to the IP address assigned to your Raritan device.

The screenshot shows the 'Add Connection' dialog box with the following configuration:

- Connect** tab selected.
- Description: Device A
- Product: Dominion KX G2
- Connection Type: TCP/IP Connection
- Find Raritan device By:
 - IP Address
 - Device Name
 - Host Name
- Use Default Port Number. Port Number: 5000

5. Select the Use Default Port Number checkbox to use the default port number (5000). For TCP Ports, devices are automatically configured to use TCP Port 5000 when communicating with the client.

If you do not want to use the default port number, deselect the checkbox and type the port number in the Port Number field.

► To modify a profile:

1. Select the device in the Navigator panel and right-click it.
2. Choose Modify Profile. The Modify Connection dialog appears.
3. Update the fields as appropriate.

4. Click OK.

► **To delete a profile:**

1. Select the device with a profile in the Navigator and right-click it.
2. Choose Delete Profile.
3. When prompted to confirm the deletion, click Yes to delete the profile for this device or click No to return to the application without deleting.

Establishing a New Connection

Note: Depending on your version of the JRE, you might receive a certificate message when using the standalone application to access a Dominion device. You have to accept the certificate in order to establish the connection.

To connect to a device, double-click the device's icon in the Navigator, then type your user name and password to connect. You can also right-click the device name in the Navigator and select New Connection.

Note: The default device login user name is admin and the default password is raritan. You have administrative privileges using these login credentials.

If you do not see an icon for your device in the Navigator, follow the instructions on creating new profiles, which is available in this section.

If you are having problems connecting to a device, be sure to check the following:

- User name - Raritan usernames *are not* case-sensitive.
 - Password - Raritan passwords *are* case-sensitive.
 - TCP Port - If you have configured your device to use a non-default TCP Port, this information must be entered into its connection profile.
 - Firewall Settings - If you are accessing a device through a firewall, that firewall must be configured to allow two-way communication on TCP Port 5000 (or the custom TCP Port to which your device has been configured).
 - Security Key - If you have configured your device to require a group security key, that key must be entered into the device's connection profile.
-

Note: If you are running MPC on Internet Explorer with both a Microsoft firewall and a non-Microsoft firewall utility installed, IE will display a message telling you that MPC is already running (even if it is not in fact running). To avoid this, deactivate one of your firewalls, or use a browser such as Mozilla or Firefox.

Connection Information▶ **To obtain information about your connection:**

- Choose Connection > Connection Info. The Connection Info dialog appears.

Generation 2 Devices

The following information is displayed about a current connection to Generation 2 devices:

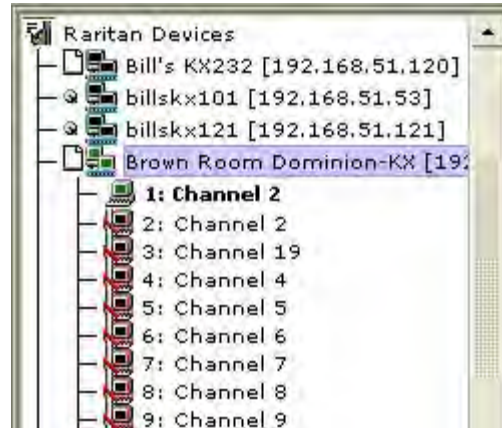
Connection information	Description
Device name	The name of your device.
IP address	The IP address of your device.
Port	The KVM Communication TCP/IP Port used to access the target device.
Data in/second	Data rate in.
Data out/second	Data rate out.
FPS	The frames per second transmitted for video.
Connect time	The duration of the connect time.
Horizontal resolution	The page resolution horizontally.
Vertical resolution	The page resolution vertically.
Refresh rate	How often the page is refreshed.
Protocol version	The RFB Protocol version.

▶ **To copy this information:**

- Click Copy to Clipboard in the Connection Info dialog. The information is now available to be pasted into the program of your choice.

Connecting to a Remote KVM Console

Once you establish a connection with a Raritan device, that device's icon in the Navigator can be expanded to display all ports enabled for remote access.



Choose one of the following options to establish a remote KVM console connection:

- Double-click the KVM port. This method closes any previous connection before connecting to the new port.
- Right-click the port and choose Switch from the shortcut menu. This method closes any previous connection before connecting to the new port.
- Right-click the port and choose New Connection from the shortcut menu. This method allows you to connect to the selected port without closing any previous connections and creates a new connection if the device supports multiple concurrent connections.

Once connected, Raritan KVM over IP devices display real-time video output of the target server (this video is compressed and encrypted according to the configuration settings specified by the administrator). You now have complete, low-level control of the KVM console as if you were physically located next to the server.

- To close a connection, right-click the connected device and choose Disconnect.
- To exit completely, choose Connection > Exit.

Closing a Remote Connection

► To close the connection:

1. Select the device in the Navigator and right-click it.
2. Choose Disconnect from the shortcut menu.

- To exit completely, click Exit on the Connection menu

Shortcut Menu

To access the shortcut menu, use either the default keyboard combination of Ctrl+Left Alt+M or the keyboard combination you assign. See **Changing the Shortcut Menu Keyboard Combination** (on page 80) for more information.

TIP: If at some point you forget the keyboard combination used to open the shortcut menu, press Ctrl+Left Alt at the same time. The keyboard combination will be displayed across the bottom of the page for five seconds.



Shortcut Menu Key Options

Execute any of the commands on the shortcut menu by either choosing the command in the menu or using a key combination. If you are using a key combination to execute a command, you will press Ctrl+Left Alt+M and then press the key on your keyboard that corresponds to the underlined letter in the shortcut menu. For example, press Ctrl+Left Alt+M+F to enter full screen mode. See the table below for information on invoking commands from the shortcut menu using keyboard combinations.

Note: You must use the Left Alt key on your keyboard when using the Ctrl+Left Alt combination.

To	Press Ctrl+Left Alt+M+
Toggle between Full/Normal screen mode*	F
Display connection information*	I
Display or set connection properties*	P
Display or set video settings*	V
Refresh the page	R
Synchronize mouse	Y
Change to/from single/double cursor mode	S
Send Ctrl+Alt+Del to the target system	D
Connect Drive	T
Connect CD-ROM/ISO Image	E
Send Ctrl+Alt+M to the target system	N
Exit a dialog or menu without altering the keyboard state	Esc

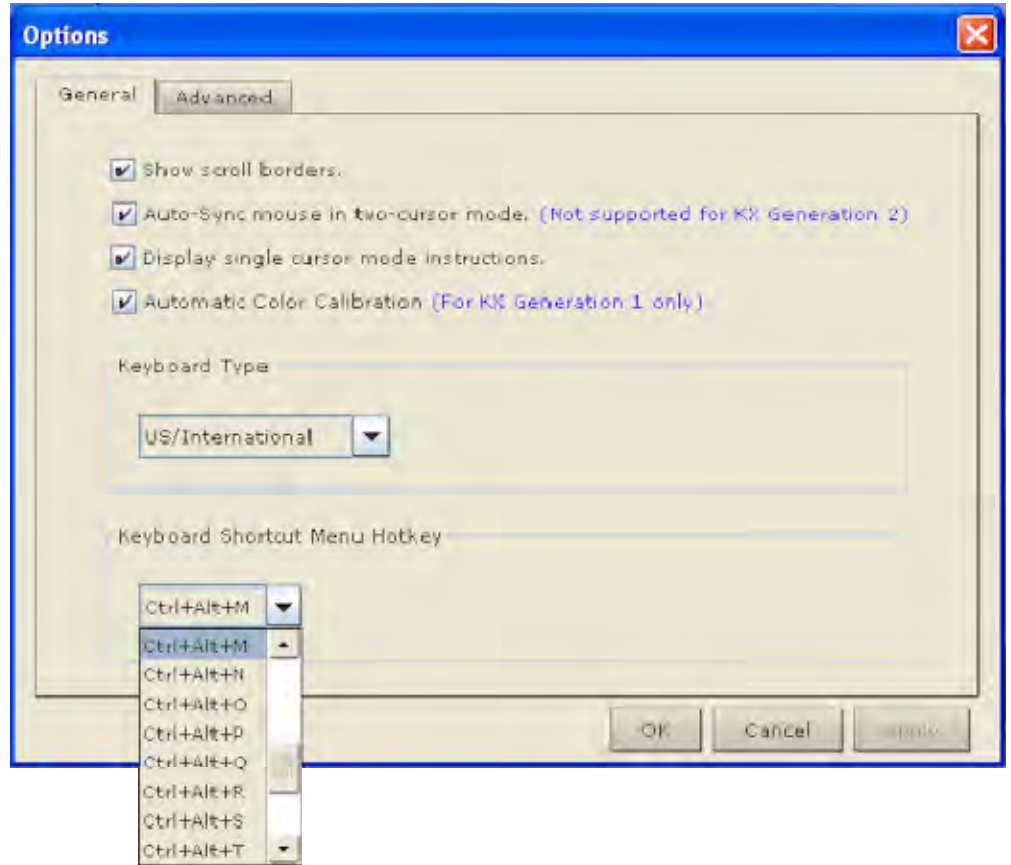
* If full screen mode is active, executing this command will automatically end full screen mode.

Changing the Shortcut Menu Keyboard Combination

► **To change the keyboard combination, do the following:**

1. Choose Tools > Options to open the Options dialog.
2. From the Keyboard Shortcut Menu HotKey drop-down, select the keyboard combination you want to use to open the shortcut menu.
3. Click OK or Apply.

Once a new keyboard combination is assigned, the new combination will be displayed in the shortcut menu and in the onscreen message that displays when the combination is used.



Keyboard Macros

A hot key combination is a set of keystrokes that performs an action when pressed. For example, the hot key combination Ctrl+Alt+0 might be created to minimize all windows.

A keyboard macro is a shortcut that sends a hot key combination to a target server. Using keyboard macros ensures that hot key combinations intended to be used on the target server are sent to and interpreted only by the target server, and not by the computer on which the client is running.

Raritan strongly suggests the use of keyboard macros instead of hot key combinations since certain hot key combinations have been found not to work properly, depending on the platform and behavioral difference between the application and web browser version. Specifically, using hot keys can result in your own client PC intercepting the command and performing the action instead of sending the command to the target server as intended.

Note: In MPC, foreign keyboard layouts are not supported when using keyboard macros, except for those keys listed in the Add Keyboard Macro dialog for Japanese and Korean.

Building a Keyboard Macro

► To build a macro:

1. Click Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.
2. Click Add. The Add Keyboard Macro dialog then appears.
3. Type a name for the macro in the Keyboard Macro Name field. This name will appear in the Keyboard menu after it is created.
4. From the Hot-Key Combination field, select a keyboard combination from the drop-down list. This allows you to execute the macro with a predefined keystroke. **Optional**
5. In the Keys to Press drop-down list:
 - a. Select each key you would like to use to emulate keystrokes. Select the keys in the order by which they are to be pressed.
 - b. After each selection, select Press Key. As each key is selected, it will appear in the Keys to Release field.

For example, select the Windows key and the letter D key. When these keys are selected in the client, the macro will be executed. Add a key release attribute to the macro if needed (see next step).

6. In the Keys to Release field:
 - a. Choose each key for which you would like to emulate a key release. Define the keys you want released in order to run the macro.

For example, specify that the keys to be pressed must also be released in order for the macro to be executed. Select the keys in the order by which they are to be released.

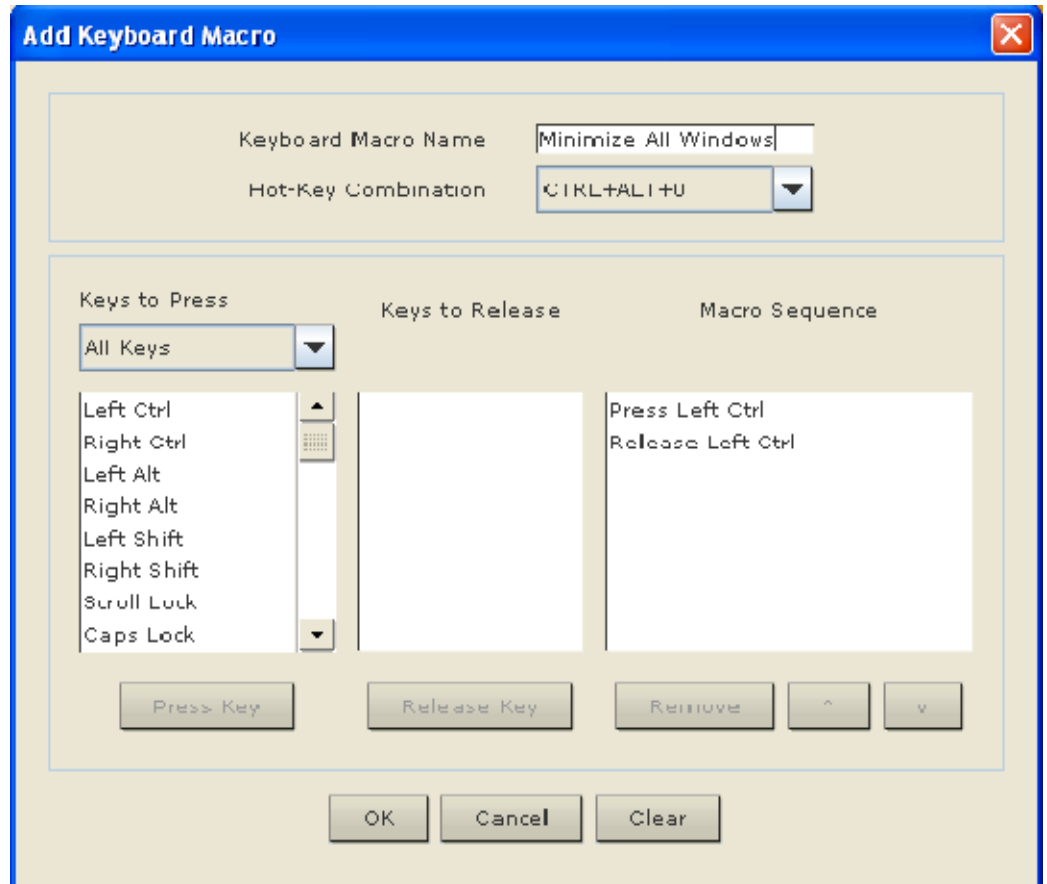
- b. Click Release Key after each selection.

7. Review the Macro Sequence field to be sure the macro sequence is defined correctly.

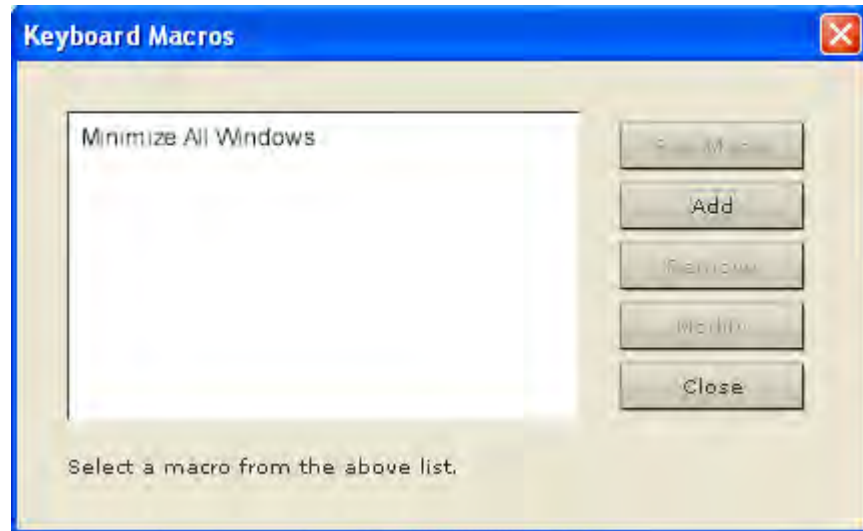
The contents of this field are automatically generated and are based on the selections made in the Keys to Press and Keys to Release fields.

- a. To remove a step in the sequence, select it and click Remove.
- b. To change the order of steps in the sequence, click the step and then click the up or down arrow buttons to reorder them as needed.

8. Click OK to save the macro. Click Clear to clear all field and start over. When you click OK, the Keyboard Macros dialog appears and lists the new keyboard macro.



9. Click Close to close the Keyboard Macros dialog. The macro will now appear on the Keyboard menu in the application. Select the new macro on the menu to run it or use the keystrokes you assigned to the macro.

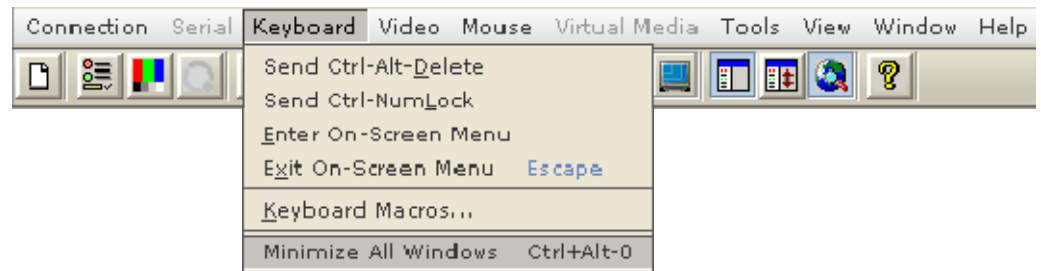


Running a Keyboard Macro

Once you have created a keyboard macro, execute it using the keyboard macro you assigned to it or by choosing it from the Keyboard menu.

Run a Macro from the Menu Bar

When you create a macro, it appears under the Keyboard menu. Execute the keyboard macro by clicking on it in the Keyboard menu.



Run a Macro Using a Keyboard Combination

If you assigned a keyboard combination to a macro when building it, you can execute the macro by pressing its assigned keystrokes. For example, press the keys Ctrl+Alt+0 simultaneously to minimize all windows on a Windows target server.

Modifying and Removing Keyboard Macros

► **To modify a macro:**


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

► **To remove a macro:**

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

Ctrl+Alt+Del Macro

Due to its frequent use, a Ctrl+Alt+Delete macro, used to reboot the target computer, has been preprogrammed. Clicking on the

Ctrl+Alt+Delete button  in the toolbar sends this key sequence to the server or to the KVM switch to which you are currently connected.

In contrast, if you were to physically press the Ctrl+Alt+Del keys, the command would first be intercepted by your own PC due to the structure of the Windows operating system, instead of sending the key sequence to the target server as intended.

Common Hot Key Exceptions for MPC


The following common hot key combinations are *not* sent to the target system:

Hot Key Combination	Description
Ctrl+Alt+Delete	Reboots the computer. The sequence is sent to the local system and the Windows Security (Task Manager, Shutdown, and so on) dialog is displayed.
Ctrl+Left Alt+M	Brings up the shortcut menu (on page 79).
Print Scrn	Treated locally and copies the page to the clipboard.

Following are limitations to specific keyboards and hot key combinations:

Hot Key Combination	Description
Alt Gr	<p>Because of a limitation in the Java Runtime Environment (JRE), Fedora, Linux, and Solaris clients receive an invalid response from Alt Gr on United Kingdom and US International language keyboards.</p> <p>Fedora, Linux, and Solaris do not pick up events for the Alt Gr key combination for Java 1.5. Java 1.6 appears to improve on this, although the keyPressed and keyReleased events for Alt Gr still identify it as an “unknown key code”.</p> <p>Further, 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.</p> <hr/> <p><i>Note: The KX II does not support Java 1.4.2.</i></p>
Alt+SysRq+[key]	<p>Since the SysRq keyboard stroke is used by some operating systems as a print shortcut, the Alt + SysRq + [key] combination is supported only as a macro when using DKX with RRC and MPC to a Linux target.</p>

Windows Key in MPC

When running MPC on a Windows JRE 1.4.2_x platform, if you press the Windows key  to display the Start menu, the Start menu will only appear on the client machine. The key is not sent to the target device.

Note: The KX II does not support Java 1.4.2.

When running MPC on a Windows JRE 1.5.0_x platform, if you press the Windows key, the Start menu appears on both the client and the target devices. Use your mouse to manually close the Start menu if you do not want to use.

Note that if you do not close the target device's Start menu properly, any key that you touch on your keyboard (that has a Windows key combination function) will send that command to the target device. For example, if you press E, the target device will open a new Explorer window. If you press D, all target windows will be minimized so you can view the desktop. To close the Start menu on the target device, click the Start button or click off of the Start menu.

Keyboard Type

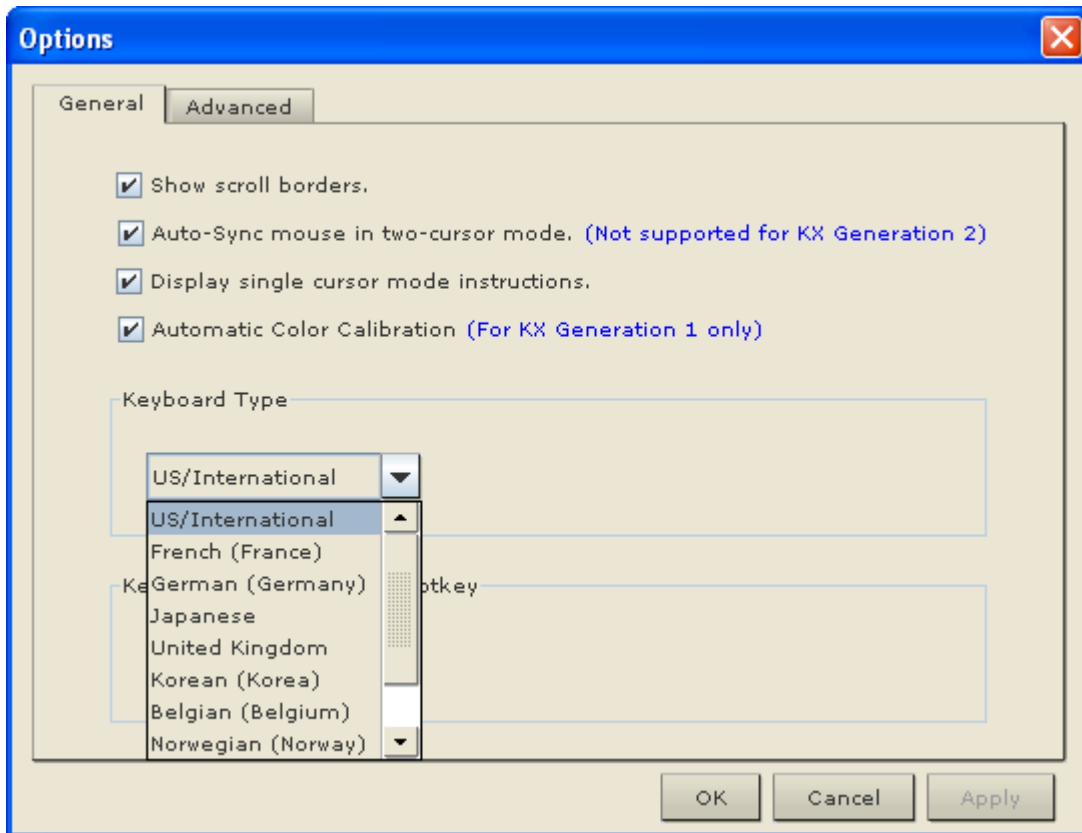
Specifying a Keyboard Type in MPC

MPC will not autodetect the type of keyboard you use, so you must specify your keyboard type to ensure accurate keyboard mapping.

► **To specify a keyboard type:**

1. Choose Tools > Options. The Options dialog will appear.
2. Click the Keyboard Type drop-down and select your keyboard type from the list.
 - US/International
 - French (France)
 - German (Germany)
 - Japanese
 - United Kingdom
 - Korean (Korea)
 - Belgian (Belgium)
 - Norwegian (Norway)
 - Danish (Denmark)
 - Swedish (Sweden)
 - German (Switzerland)
 - Hungarian (Hungary)
 - Spanish (Spain)
 - Italian (Italy)
 - Slovenian

3. Click OK.



Keyboard Limitations

Slovenian Keyboards

The < key does not work on Slovenian keyboards due to a JRE limitation.

Language Configuration on Linux

Because the Sun JRE on Linux has problems generating the correct Key Events for foreign-language keyboards configured using System Preferences, Raritan recommends that you configure foreign keyboards using the methods described in the following table.

Language	Configuration method
US Intl	Default
French	Keyboard Indicator
German	System Settings (Control Center)
Japanese	System Settings (Control Center)

Language	Configuration method
UK	System Settings (Control Center)
Korean	System Settings (Control Center)
Belgian	Keyboard Indicator
Norwegian	Keyboard Indicator
Danish	Keyboard Indicator
Swedish	Keyboard Indicator
Hungarian	System Settings (Control Center)
Spanish	System Settings (Control Center)
Italian	System Settings (Control Center)
Slovenian	System Settings (Control Center)

Note: The Keyboard Indicator should be used on Linux systems using Gnome as a desktop environment.

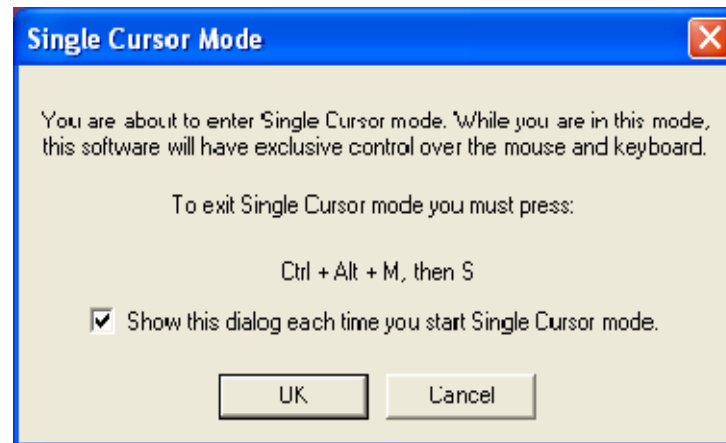
Mouse Options


Single Cursor Mode/Dual Cursor Mode

When remotely viewing a target server that uses a mouse, you will see two mouse cursors on the remote desktop. When your mouse pointer lies within the remote desktop area, mouse movements and clicks are directly transmitted to the connected target server. The pointer, generated by the operating system, slightly leads the target server's mouse pointer during movement. This is a result of digital delay.

On fast LAN connections, you may want to disable the mouse pointer and view only the target server's pointer. To toggle between these two modes, choose Single/Double Cursor on the shortcut menu.

Alternatively, click the Single Mouse Pointer icon  in the toolbar or choose Mouse > Single Cursor Mode.



When in Dual Cursor mode, press Ctrl+Left Alt+M and execute the Synchronize Mouse shortcut to force realignment of the mouse cursors. If the mouse cursors still remain out of sync, click the Auto-Sense Video Settings button  on the toolbar.

Note: When in Dual Cursor mode, if the dual mouse cursors are synchronized but left idle for five minutes or longer, the target mouse pointer will automatically align itself with the upper left corner of the target window. Execute the Synchronize Mouse command to ensure local and target mouse pointer alignment.

Single Mouse Cursor mode for Apple Mac target servers is supported for MPC. Select Single Mouse Cursor on the Mouse menu in MPC to enter this mode. While in this mode, the cursor will remain in the video window for the Mac Server. To exit, open the shortcut menu and press S on the keyboard.

Mouse Synchronization Options

In addition to synchronizing mouse cursors or toggling between single and dual cursor mode, the Mouse menu provides three options for syncing cursors when in dual cursor mode:

Menu option	Description
Absolute	When connected to selected Dominion devices and targets with USB ports, the application will use absolute coordinates to keep the cursors in sync. See Absolute Mouse Mode (on page 92) for more information.
Intelligent	Under certain conditions, the application can detect the target mouse settings and synchronize the mouse cursors accordingly, accelerating the mouse on the target device. See Intelligent Mouse Mode (on page 55) for more details.
Standard	This is the standard mouse synchronization algorithm. See Standard Mouse Mode (on page 54) for more information.

Note: The Intelligent and Standard Mouse modes are available to all KX II-101 targets. Absolute Mouse mode are only available to Mac and Windows USB targets.

Absolute Mouse Mode

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

► **To enter absolute mouse mode:**

- Choose Mouse > Absolute.

Note: The absolute mouse setting requires a USB target system and is the recommended mouse setting for KX II-101.

Intelligent Mouse Mode

In Intelligent Mouse mode, the KX II-101 device can detect the target mouse settings and synchronize the mouse cursors 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.

► To enter intelligent mouse mode:

- Choose Mouse > Intelligent.

Intelligent Mouse Synchronization Conditions

The Intelligent Mouse Synchronization command, available on the Mouse menu, automatically synchronizes mouse cursors during moments of inactivity. For this to work properly, however, the following conditions must be met:

- The active desktop should be disabled on the target.
- No windows should appear in the top left corner of the target page.
- There should not be an animated background in the top left corner of the target page.
- The target mouse cursor shape should be normal and not animated.
- The target mouse speeds should not be set to very slow or very high values.
- Advanced mouse properties such as “Enhanced pointer precision” or “Snap mouse to default button in dialogs” should be disabled.
- Choose “Best Possible Video Mode” in the Video Settings window.
- The edges of the target video should be clearly visible (that is, a black border should be visible between the target desktop and the remote KVM console window when you scroll to an edge of the target video image).
- When using the intelligent mouse synchronization function, having a file icon or folder icon located in the upper left corner of your desktop may cause the function not to work properly. To be sure to avoid any problems with this function, Raritan recommends you do not have file icons or folder icons in the upper left corner of your desktop.

After autosensing the target video, manually initiate mouse synchronization by clicking the Synchronize Mouse button on the toolbar. This also applies when the resolution of the target changes if the mouse cursors start to desync from each other.

If intelligent mouse synchronization fails, this mode will revert to standard mouse synchronization behavior.

Please note that mouse configurations will vary on different target operating systems. Consult your OS guidelines for further details. Also note that intelligent mouse synchronization does not work with UNIX targets.

Standard Mouse Mode

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

► **To enter standard mouse mode:**

- Choose Mouse > Standard.


Connection and Video Properties

Dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. The KX II-101 device optimizes KVM output not only for LAN use but also for WAN and dial-up use. These devices can also control color depth and limit video output, offering an optimal balance between video quality and system responsiveness for any bandwidth constraint.

The parameters discussed in this section can be optimized in the Connection Properties dialog and Video Settings dialog.

MPC Connection Properties

► **To adjust connection properties:**

1. Choose Connection > Properties or click the Connection Properties button  in the toolbar. Update the settings in the Compression tab.
2. Set the Connection Speed.

Use this setting to manually adjust the connection speed to accommodate bandwidth constraints. Devices can automatically detect available bandwidth and not limit bandwidth use. However, you can also adjust this usage according to your needs. Depending on the Raritan device in use, different options may be available:

- Auto Detect
- 100mb Ethernet
- 10mb Ethernet
- 1.5mb (Max DSL/T1)
- 1mb (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)
3. Set the Color Depth.

Devices can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths. Select from among the options in the drop-down list. Depending on the Raritan device in use, different options may be available:


- 15-bit RGB Color
- 8-bit RGB Color
- 4-bit Color
- 4-bit Gray
- 3-bit Gray
- 2-bit Gray
- Black and White

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

4. Use the slider to select the desired level of video Smoothing (15-bit mode only). The level determines how aggressively to blend page regions with small color variation into a single, smooth color. Smoothing improves the appearance of the target video by reducing the video noise that is displayed.
5. Click OK to create the connection profile.

Video Settings - Generation 2 Devices

► To configure Generation 1 devices:

1. Choose Video > Video Settings or click the Video Settings button  in the toolbar to open the Settings dialog.
2. Adjust the following settings as required:
 - a. Noise Filter

Devices 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 page changes. Lower settings transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.

Note: The default Noise Filter is 4. Raritan recommends that you lower this value to 0 (zero). Although higher settings will stop the needless transmission of false color variations, true and intentional small changes to a video image may not be transmitted.

b. PLL Settings

If the video image looks extremely blurry or unfocused, the PLL settings for clock and phase can be adjusted until a better image appears on the active target server.

Warning: Exercise caution when changing the clock and phase settings since 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 page. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended. Under most circumstances this setting should not be changed because the autodetect is usually quite accurate.
- Phase - Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.

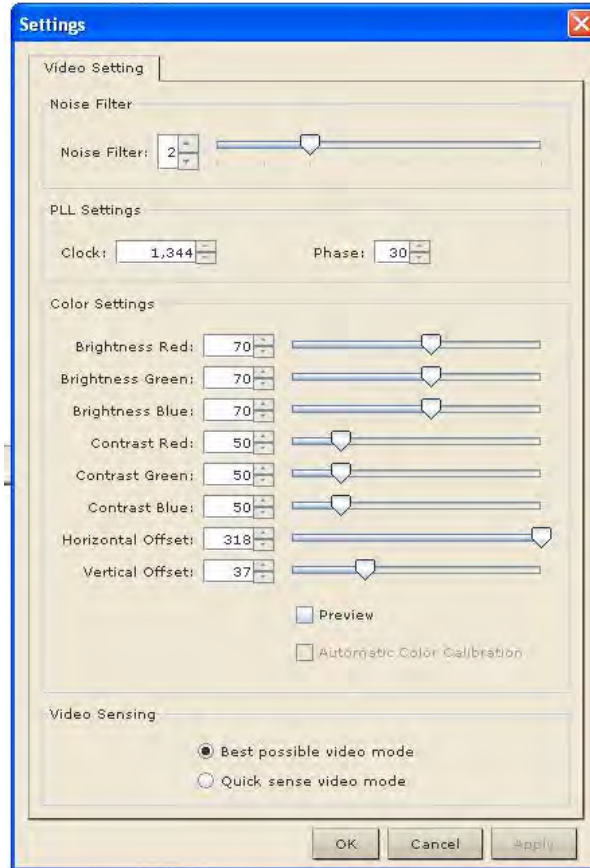
a. Color Settings

These settings control the brightness, contrast, and positioning of the target server display. Select the Link Color Controls checkbox to make all slide adjusters move in unison when any one option is moved.

- Brightness Red - Controls the brightness of the red signal; range is 0 - 127.
- Brightness Green - Controls the brightness of the green signal; range is 0 - 127.
- Brightness Blue - Controls the brightness of the blue signal; range is 0 - 127.
- Contrast Red - Controls the red signal contrast; range is 0 - 255.
- Contrast Green - Controls the green signal contrast; range is 0 - 255.

- Contrast Blue - Controls the blue signal contrast; range is 0 - 255.
 - Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor; range is 0 - 512.
 - Vertical Offset - Controls the vertical positioning of the target server display on your monitor; range is 0 - 128.
3. To preview the change prior to making the selection, check the Preview checkbox.
 4. Check the Automatic Color Calibration checkbox to enable this feature.
 5. Select the video sensing mode:
 - Best possible video mode - Devices 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 - Selecting this option will cause the device to 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.

6. Click OK to apply the settings and close the dialog. Click Apply to apply the settings without closing the dialog.

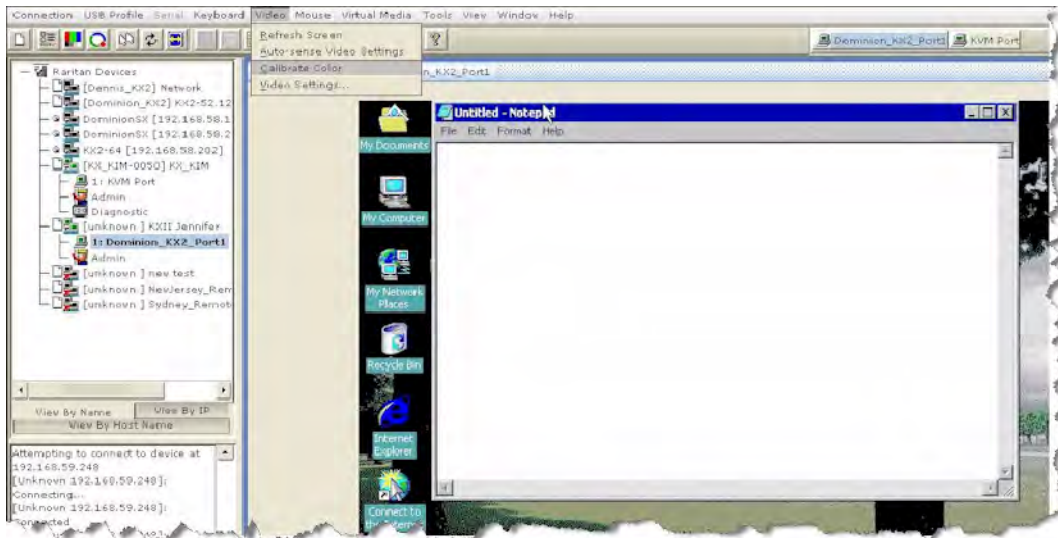



Color Calibration

Use the Color Calibration command if the color levels (hue, brightness, and saturation) of the transmitted video images do not seem accurate. The device color settings remain the same when switching from one target KVM server to another, so you can perform color calibration once to affect all connected target servers.

1. Open a remote KVM connection to any server running a graphical user interface.
2. Ensure that a solid white color covers approximately 15% or more of the target server's desktop.

TIP: Open Microsoft Notepad and maximize the window.



3. On the Video menu, choose Calibrate Color or click the Color Calibration button  on the toolbar. The target device page will update its calibration.

*Tip: You can also specify automatic color calibration using Tools > Options. See **General Options in MPC** (on page 100) for more information.*

Administrative Functions

Although your device provides a remote interface to administrative functions through the device manager, the client provides an interface to frequently-used administrative functions directly from its own interface. When logged into a device as an administrator, you can perform the administrative tasks discussed here.

Note: Most of the commands discussed here are available in both the Tools menu and in the shortcut menu that appears when you right-click the device in the Navigator panel.

Note to MPC Users

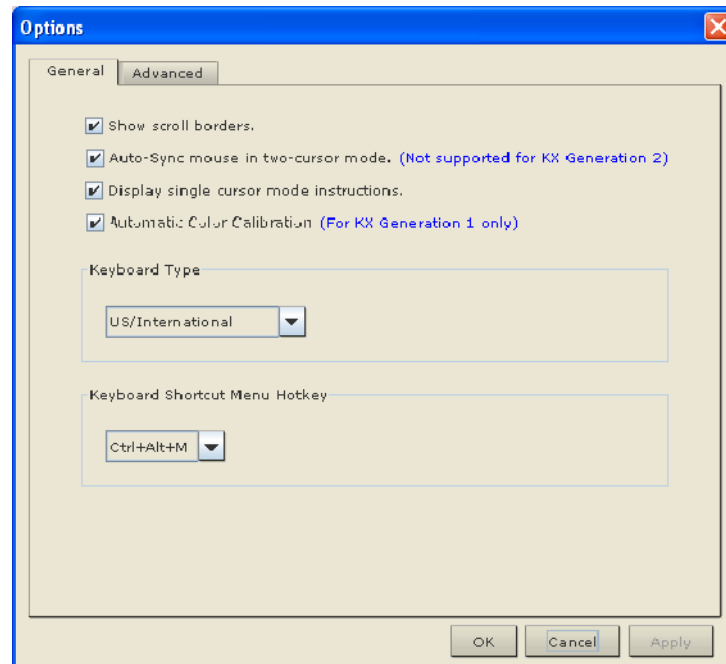
MPC users must belong to the Administrator group in order to receive administrative permissions. MPC uses one permission: either Administrator or Normal User. It is only when the user belongs to the Administrator group that they have access to backup, restore, and restart functions. This is true regardless of any device user group settings that may be applied to the user.

General Options in MPC

The Options available in the Tools menu provide options that allow you to customize scroll borders, mouse mode settings, single cursor mode, auto color calibration, hot key configuration, keyboard type, broadcast port, and logging.

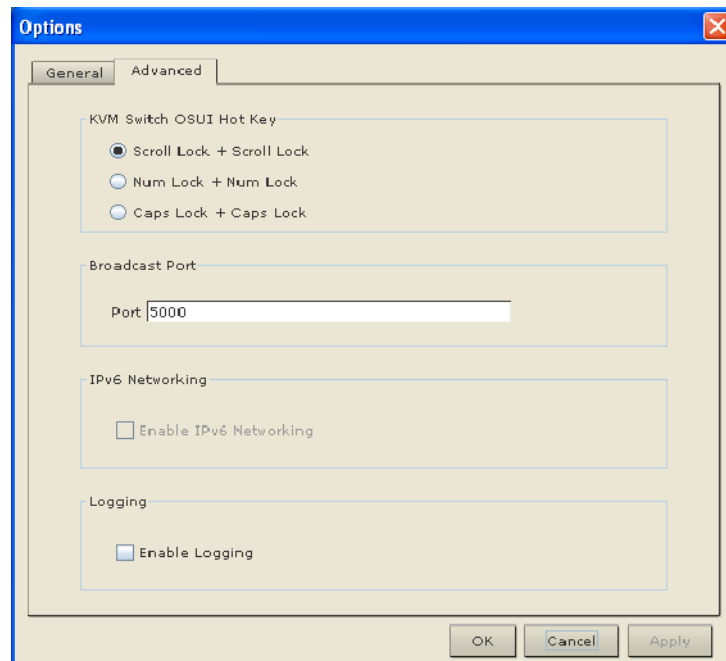
► **To configure the general options in MPC:**

1. Choose Tools > Options. The Options dialog appears and displays the General tab by default.



2. Select the "Show scroll borders" checkbox to view the thin scroll borders designating the autoscroll area.
3. Select the "Auto-Sync mouse in two-cursor mode" checkbox to enable automatic mouse synchronization.
4. If you select the "Display single cursor mode instructions" checkbox, the Single Cursor Mode dialog will appear each time Single Cursor is enabled in the application. See **Mouse Options** (on page 91) for more information.
5. Select the Automatic Color Calibration checkbox to enable automatic color calibration. This option is available for KX generation 1 (G1) only.
6. Select the Keyboard Type from the drop-down list (depending on the Raritan device in use, different options may be available):
 - US/International

- French (France)
 - German (Germany)
 - Japanese
 - United Kingdom
 - Korean (Korea)
 - Belgian (Belgium)
 - Norwegian (Norway)
 - Danish (Denmark)
 - Swedish (Sweden)
 - German (Switzerland)
 - Hungarian (Hungary)
 - Spanish (Spain)
 - Italian (Italy)
 - Slovenian
7. From the Keyboard Shortcut Menu HotKey drop-down, select the key combination you would like to use to invoke the **Shortcut Menu** (on page 79).
 8. For advanced options, open the Advanced tab.



9. From the KVM Switch OSUI Hot Key section, select the hot key to use when switching between target server displays.

10. For the Broadcast Port, type the broadcast port number in the Port field if you want to use a port other than 5000.
11. Select the Enable IPv6 Networking checkbox for IPv6 to enable IPv4 and IPv6 dual-stack operation.

Note: KSX II and KX II-101 devices are not IPv6 enabled, so this section will not apply to those devices.

12. Select the Enable Logging checkbox only if directed to by Technical Support. This option creates a log file in your home directory.
13. Click OK when finished. Click Apply any time while making selections to apply it.

Upgrading Device Firmware

► **To update a device's firmware:**

1. Connect to the device by highlighting the device's icon in the Navigator.
2. Click Tools > Update > Update Device to perform firmware upgrades.
3. You will be prompted to locate a Raritan firmware distribution file (*.RFP format), which can be found on the Raritan website (www.raritan.com) on the Firmware Upgrades page.

Ensure that you read all instructions included in Firmware Upgrade Guide carefully before upgrading a device.

Note: Copy the firmware update file on the Raritan website to a local machine before uploading. Do not load the file from a network drive.

Changing a Password

► **To update your password**

1. Connect to a target by selecting it in the Navigator.

- Highlight the target's icon in the Navigator and then choose Tools > Update > User Password. The Change Password dialog appears.



- Type your current password in the Old Password field.
- Type the new password in the New Password field.
- Retype the password in the Confirm New Password field.
- When finished, click OK.

Restarting a Device

► To restart a device:

- Select the device in the Navigator.
- On the Tools menu, choose Restart Device.

Backup and Restore Functions

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 from another Dominion device to your team by backing up the user configuration settings from the device in use and restoring those configurations to the new Dominion device.

Backing Up and Restoring a Device Configuration

► To back up a device:

- Download the device configuration to your local computer by selecting the device in the Navigator.
- Click Tools > Save Device Configuration.

► To restore a device configuration:

- Upload the archived device configuration by selecting the device in the Navigator.

2. Click Tools > Restore Device Configuration.

Note that device configuration is specific to a particular device and should not be restored to another device.

Backing Up and Restoring a User Configuration

▶ **To back up a device's user configuration:**

1. Select the device in the Navigator.
2. Click Tools > Save User Configuration.

▶ **To restore a user configuration:**

1. Upload a device's archived user configuration by selecting the device in the Navigator.
2. Click Tools > Restore User Configuration.

Note: Use these commands to easily transfer user and group information from one device to another.

Broadcast Port

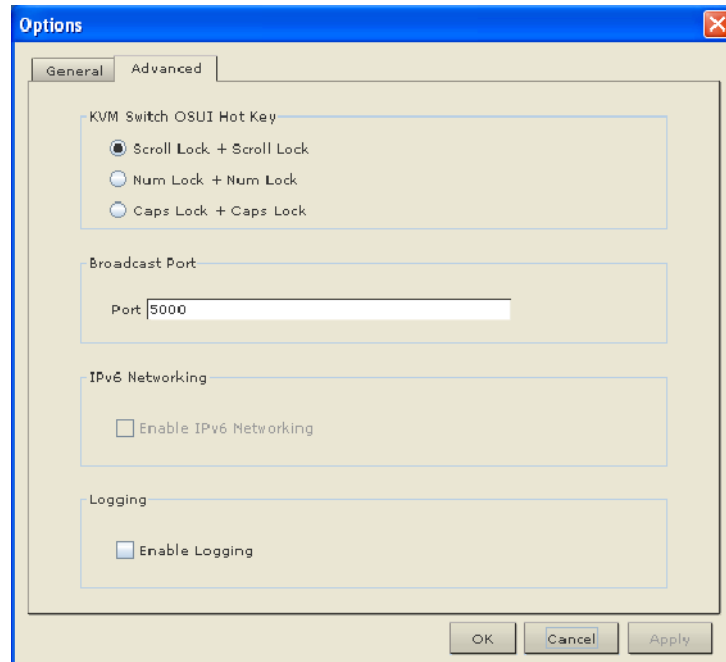
By default, all Raritan devices send data through Port 5000. This network traffic includes the autodiscovery broadcast. In the case of conflicts or to deal with firewall issues, you may want to use a different broadcast port.

MPC Broadcast Port

▶ **To change the autodiscovery port from the default broadcast port of 5000:**

1. Select the device in the Navigator.
2. Choose Tools > Options. The Options dialog appears.
3. On the Advanced tab, type the new port number in the Port field of the Broadcast Port section and then click OK.

Note: If you want the application to autodiscover Raritan devices on the new broadcast port you entered in the Options dialog, you must configure all Raritan devices to use the new port number.



Remote Power Management

AC power to associated targets can be managed when used with a properly configured Raritan Remote Power Control Strip (RPC strip). Three options are available when performing remote target power management:

- Power On
- Power Off
- Cycle Power

► To change the power status of a target:

1. Select the device in the Navigator.
2. On the Tools menu, choose Power On, Power Off, or Cycle Power.

Chapter 4 Virtual Media

In This Chapter

Overview	107
Prerequisites for Using Virtual Media	110
File Server Setup (File Server ISO Images Only)	111
Connecting to Virtual Media	113
Disconnecting Virtual Media	115

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 floppy drives, and ISO images (disk images).

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 (if supported by machine BIOS)

This expanded KVM control eliminates most trips to the data center, saving time and money.

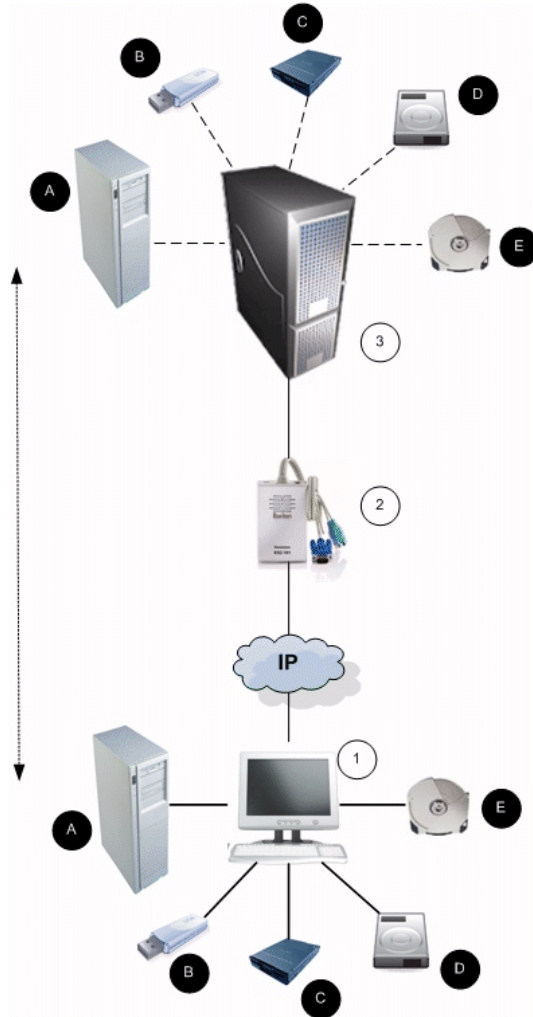


Diagram key	
1	Local workstation
2	KX II-101
3	Target server
A	Remote file server (ISO images)
B	USB drive
C	Floppy drive
D	CD/DVD drive
E	Hard drive image files

Prerequisites for Using Virtual Media

With the KX II-101 virtual media feature, you can mount up to two drives (of different types) that are supported by the USB profile currently applied to the target. These drives are accessible for the duration of the KVM session.

For example, you can mount a specific CD-ROM, use it, and then disconnect it when you are done. The CD-ROM virtual media “channel” will remain open, however, so that you can virtually mount another CD-ROM. These virtual media “channels” remain open until the KVM session is closed as long as the USB profile supports it.

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

KX II-101

- For users requiring access to virtual media, the KX II-101 device 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.
- If you want to use PC-Share, Security Settings must also be enabled in the Security Settings page. **Optional**

Client PC

- Certain virtual media options require administrative privileges on the client PC (for example, 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 the Start Menu, locate IE, right-click it and select Run as Administrator.

Target Server

- KVM target servers must support USB connected drives.
- KVM target servers running Windows 2000 must have all of the recent patches installed.
- USB 2.0 ports are both faster and preferred.

▶ To use virtual media:

- Connect/attach the media to the client or network file server that you want to access from the target server. This need not be the first step, but it must be done prior to attempting to access this media.

File Server Setup (File Server ISO Images Only)

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

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

Use the KX II-101 Remote Console File Server Setup page to designate the files server(s) and image paths that you want to access using KX II-101 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 KX II-101 Remote Console. The File Server Setup page opens.
2. Check the Selected checkbox for all media that you want accessible as virtual media.
3. Enter information about the file server ISO images that you want to access:
 - IP Address/Host Name - Host name or IP address of the file server.
 - Image Path - Full path name of the location of the ISO image.

Note: The host name cannot exceed 232 characters in length.

4. Click Save. All media specified here will now be available for selection in the Map Virtual Media CD/ISO Image dialog.

Form > File Server Setup

File Server Setup

IP Address/Host Name: Enter name of the host name or IP Address of shared drive containing ".iso" image.
Image Path: Enter path to ".iso" image on shared drive. Do not include host name or IP Address in the path.

Selected	IP Address/Host Name	Image Path
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<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

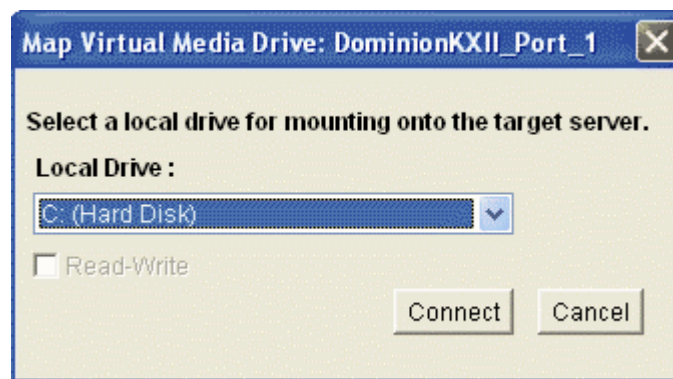
Connecting to Virtual Media

Local Drives

This option mounts an entire drive, which means the entire disk drive is mounted virtually onto the target server. Use this option for hard drives and external drives only. It does not include network drives, CD-ROM, or DVD-ROM drives. This is the only option for which Read/Write is available.

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

1. From the Virtual KVM Client, choose Virtual Media > Connect Drive. The Map Virtual Media Drive dialog appears.



2. Choose the drive from the Local Drive drop-down list.
3. If you want Read and Write capabilities, select the Read-Write checkbox. This option is disabled for nonremovable drives. See the **Conditions when Read/Write is Not Available** (on page 114) for more information. When checked, you will be able to read or write to the connected USB disk.

WARNING: Enabling Read/Write access can be dangerous! Simultaneous access to the same drive from more than one entity can result in data corruption. If you do not require Write access, leave this option unselected.

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

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.

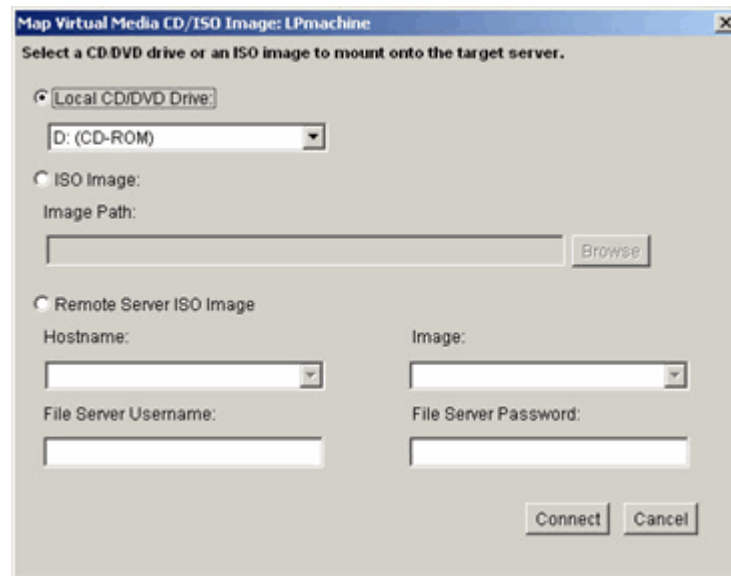
CD-ROM/DVD-ROM/ISO Images

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 appears.



2. For internal and external CD-ROM or DVD-ROM drives:
 - a. Choose the Local CD/DVD Drive option.
 - b. Choose the drive from the Local CD/DVD Drive drop-down list. All available internal and external CD and DVD drive names will be populated in the drop-down list.

- c. Click Connect.
3. For ISO images:
 - a. Choose the ISO Image option. Use this option when you want to access a disk image of a CD, DVD, or hard drive. ISO format is the only format supported.
 - b. Click 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 KX II-101 File Server Setup page will be in the drop-down list. See **File Server Setup (File Server ISO Images Only)** (on page 111) for more information.
 - c. File Server Username - User name 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.

Note: If you are working with files on a Linux target, use the Linux Sync command after the files are copied using virtual media in order to view the copied files. Files may not appear until a sync is performed.

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 command, simply closing the KVM connection closes the virtual media as well.

Chapter 5 User Management

In This Chapter

User Groups	116
Users	123
Authentication Settings.....	126
Changing a Password	137

User Groups

Every KX II-101 is delivered with three default user groups. These groups cannot be deleted:

User	Description
Admin	Users that are members of this group have full administrative privileges. The original, factory-default user is a member of this group and has the complete set of system privileges. In addition, the Admin user must be a member of the Admin group.
Unknown	This is the default group for users who are authenticated externally using LDAP/LDAPS or RADIUS or who are unknown to the system. If the external LDAP/LDAPS or RADIUS server does not identify a valid user group, the Unknown group is used. In addition, any newly created user is automatically put in this group until assigned to another group.
Individual Group	An individual group is essentially a “group” of one. That is, the specific user is in its own group, not affiliated with other real groups. Individual groups can be identified by the “@” in the Group Name. The individual group allows a user account to have the same rights as a group.

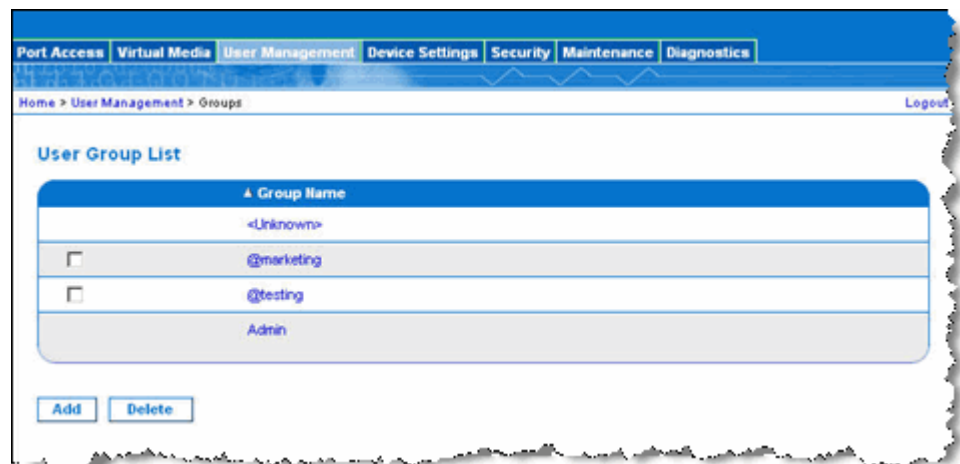
User Group List

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

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

► To list the user groups:

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



Relationship Between Users and Groups

Users belong to a group and groups have privileges. Organizing the various users of your KX II-101 into groups saves time by allowing you to manage permissions for all users in a group at once, instead of managing permissions on a user-by-user basis.

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

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

Adding a New User Group

► **To add a new user group:**

1. Open the Group page by selecting User Management > Add New User Group or clicking the Add button from the User Group List page.

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

2. Type a descriptive name for the new user group into the Group Name field (up to 30 characters).
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. See **Setting Permissions** (on page 122).
4. Set the port permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). See **Setting Port Permissions** (on page 119).
5. Set the IP ACL. See **Group-Based IP ACL (Access Control List)** (on page 120). This feature limits access to the KX II-101 device by specifying IP addresses. It applies only to users belonging to a specific group, unlike the IP Access Control list feature that applies to all access attempts to the device (and takes priority). **Optional**

6. Click OK.

Home > User Management > Group

Group

Group Name *

▼ Permissions

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

▼ Port Permissions

Port	Access	VM Access	Power Control
1: Dominion_KX2_101_Port1	Deny	Deny	Deny
2: Power Port 1	Deny		Deny

▼ IP ACL

Rule #	Starting IP	Ending IP	Action
			ACCEPT

Append Insert Replace Delete

OK Cancel

© 2008 Raritan, Inc.

Setting Port Permissions

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

Port Access	
Option	Description
Deny	Denied access completely
View	View the video (but not interact with) the connected target server
Control	Control the connected target server. Control must be assigned to the group if VM and power control access will also be granted.

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

Power control access	
Option	Description
Deny	Deny power control to the target server
Access	Full permission to power control on a target server

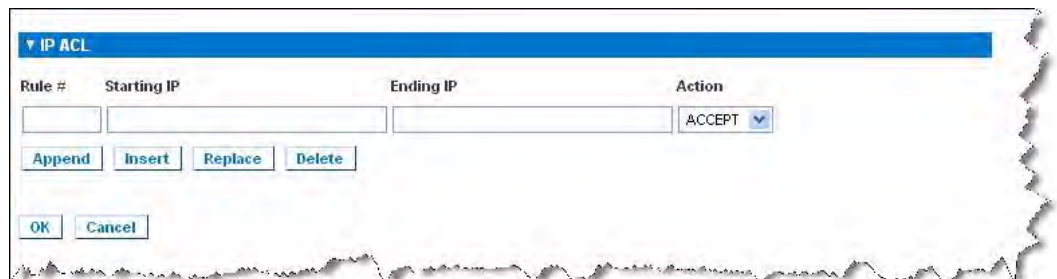
Group-Based IP ACL (Access Control List)

Important: Exercise caution when using group-based IP access control. It is possible to be locked out of your KX II-101 if your IP address is within a range that has been denied access.

This feature limits access to the KX II-101 device by users in the selected group to specific IP addresses. This feature applies only to users belonging to a specific group, unlike the IP Access Control List feature that applies to all access attempts to the device, is processed first, and takes priority.

Important: The IP address 127.0.0.1 is used by the KX II-101 Local Port and cannot be blocked.

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



▶ **To add (append) rules:**

1. Type the starting IP address in the Starting IP field.
2. Type the ending IP address in the Ending IP field.
3. Choose the action from the available options:
 - Accept - IP addresses set to Accept are allowed access to the KX II-101 device.
 - Drop - IP addresses set to Drop are denied access to the KX II-101 device.
4. Click Append. The rule is added to the bottom of the rules list. Repeat steps 1 through 4 for each rule you want to enter.

▶ **To insert a rule:**

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

▶ **To replace a rule:**

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

▶ **To delete a rule:**

1. Specify the rule number you want to delete.
2. Click Delete.
3. When prompted to confirm the deletion, click OK.

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

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

Setting Permissions

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

Permission	Description
Device 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, KX II-101 diagnostics
Maintenance	Backup and restore database, firmware upgrade, factory reset, reboot
PC-Share	Simultaneous access to the same target by multiple users
Security	SSL certificate, security settings (VM Share, PC-Share), IP ACL
User Management	User and group management, remote authentication (LDAP/LDAPS/RADIUS), login settings

Setting Permissions for an Individual Group

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

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

Modifying an 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.
2. Set the Permissions for the group. Select the checkboxes before the permissions you want to assign to all of the users belonging to this group. See **Setting Permissions** (on page 122).
3. Set the Port Permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). See **Setting Port Permissions** (on page 119).
4. Set the IP ACL (optional). This feature limits access to the KX II-101 device by specifying IP addresses. See **Group-Based IP ACL (Access Control List)** (on page 120).
5. Click OK.

► **To delete a user group:**

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

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

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

Users

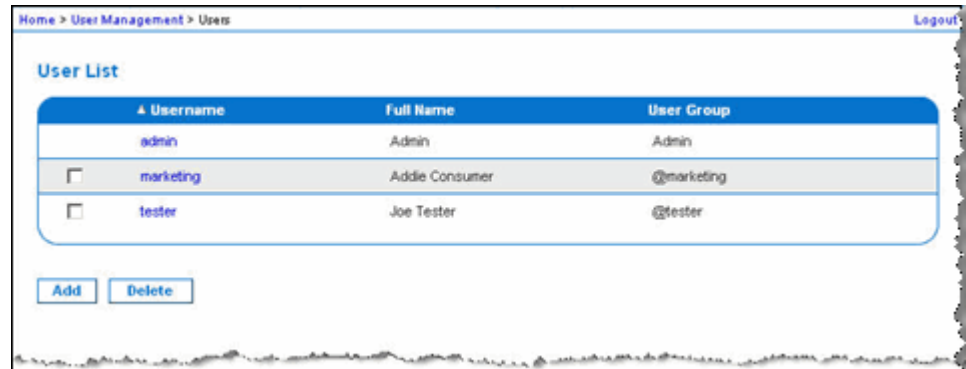
Users must be granted user names and passwords to gain access to the KX II-101. This information is used to authenticate users attempting to access your KX II-101.

User List

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

► **To view the list of users:**

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



Adding a New User

It is a good idea to define user groups before creating KX II-101 users because, when you add a user, you must assign that user to an existing user group. See **Adding a New User Group** (on page 118).

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

*Note: A user name can be deactivated when the number of failed login attempts has exceeded the maximum login attempts set in the Security Settings page. See **Security Settings** (on page 184).*

► **To add a new user:**

1. Open the User page by choosing User Management > Add New User or clicking the Add button on the User List page.
2. Type a unique name in the Username field (up to 16 characters).
3. Type the person's full name in the Full Name field (up to 64 characters).
4. Type a password in the Password field and retype the password in the Confirm Password field (up to 64 characters).

5. 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>, which is the 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, see **Setting Permissions for an Individual Group** (on page 122).

6. To activate the new user, select the Active checkbox. The default is activated (enabled).
7. Click OK.

Modifying an Existing User

► **To modify an existing user:**

1. Locate the user from among those listed on the User List page.
2. Click the user name. The User page opens.
3. On the User page, change the appropriate fields. (See **Adding a New User** (on page 124) for information about how to get access the User page.)
4. To delete a user, click Delete. You are prompted to confirm the deletion.
5. Click OK.

Blocking and Unblocking Users

A user's access to the system can be blocked by the administrator or automatically blocked based on security settings. See **User Blocking** (on page 188). A blocked user becomes inactive and can be unblocked by being made active again by the administrator.

► **To block or unblock a user:**

1. Choose User Management > User List. The User List page opens.
2. Select or deselect the Active checkbox.
 - If selected, the user is made active and given access to the KX II-101.
 - If deselected, the user is made inactive and cannot access the KX II-101.
3. Click OK. The user's active status is updated.

Authentication Settings

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

When the KX II-101 is configured for remote authentication, the external authentication server is used primarily for the purposes of authentication, not authorization.

From the Authentication Settings page you can configure the type of authentication used for access to your KX II-101.

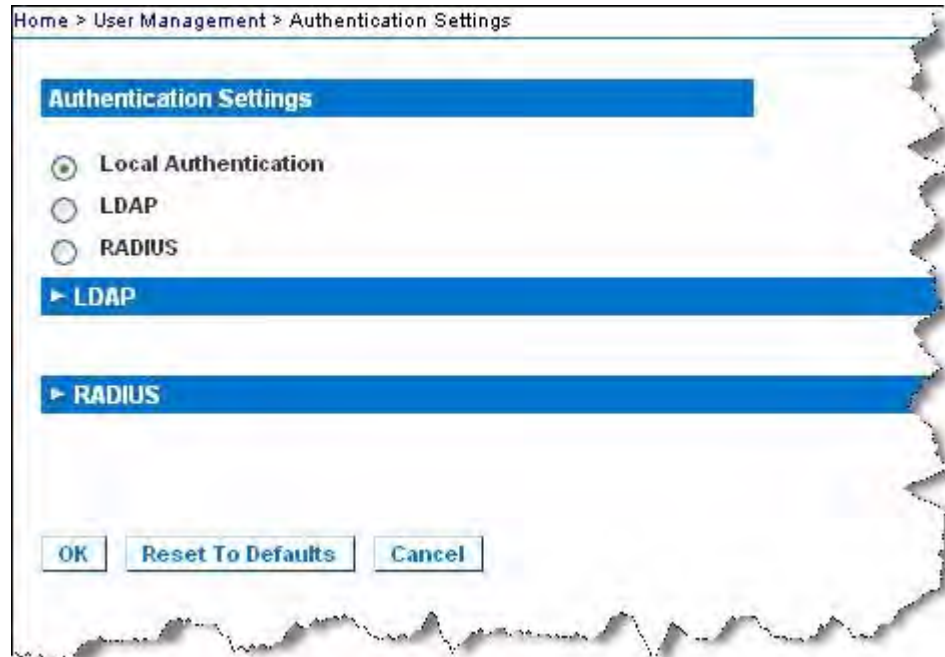
Note: Even if you select remote authentication (LDAP/LDAPS or RADIUS), local authentication is still used.

► **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 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 130) for information about completing the fields in the RADIUS section of the Authentication Settings page.
6. Click OK to save.

► **To return to factory defaults:**

- Click the Reset to Defaults button.




Implementing LDAP/LDAPS Remote Authentication

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

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

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

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

4. In the Primary LDAP Server field, type the IP address or DNS name of your LDAP/LDAPS remote authentication server (up to 37 characters). When the Enable Secure LDAP option is selected, the DNS name must be used.
5. In the Secondary LDAP Server field, type the IP address or DNS name of your backup LDAP/LDAPS server (up to 37 characters). When the Enable Secure LDAP option is selected, the DNS name must be used. Note that the remaining fields share the same settings with the Primary LDAP Server field. **Optional**
6. In the Secret Phrase field and again in the Confirm Secret Phrase field, type the server secret (password) required to authenticate against your remote authentication server (up to 45 characters). Enter the password in use on the LDAP/LDAPS server.
7. Select the Enable Secure LDAP checkbox if you would like to use SSL. This will enable the Secure LDAP Port field. Secure Sockets Layer (SSL) is a cryptographic protocol that allows KX II-101 to communicate securely with the LDAP/LDAPS server.
8. The default Port is 389. Either use the standard LDAP TCP port or specify another port.
9. 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.
10. 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.
11. DN of Administrative User - Distinguished Name of administrative user (up to 31 characters). 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.`
12. User Search DN - Enter the name you want to bind against the LDAP/LDAPS (up to 31 characters), 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.
13. 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.

14. Active Directory Domain. Type the name of the Active Directory Domain.

The screenshot shows the 'Authentication Settings' page in a web browser. The breadcrumb trail is 'Home > User Management > Authentication Settings'. The page title is 'Authentication Settings'. There are three radio button options: 'Local Authentication', 'LDAP' (which is selected), and 'RADIUS'. Below these is a blue bar with a downward arrow and the text 'LDAP'. The form contains several fields: 'Primary LDAP Server' (empty), 'Secondary LDAP Server' (empty), 'Secret Phrase' (empty), 'Confirm Secret Phrase' (empty), an unchecked checkbox for 'Enable Secure LDAP', 'Port' (389), 'Secure LDAP Port' (636), 'Certificate File' (empty with a 'Browse...' button), 'DN of Administrative User' (empty), 'User Search DN' (empty), 'Type of External LDAP Server' (dropdown menu set to 'Generic LDAP server'), and 'Active Directory Domain' (empty).

Returning User Group Information from Active Directory Server

The KX II-101 supports user authentication to Active Directory (AD) without requiring that users be defined locally on the KX II-101. This allows Active Directory user accounts and passwords to be maintained exclusively on the AD server. Authorization and AD user privileges are controlled and administered through the standard KX II-101 policies and user group privileges that are applied locally to AD user groups.

IMPORTANT: If you are an existing Raritan, Inc. customer, and have already configured the Active Directory server by changing the AD schema, the KX II-101 still supports this configuration and you do not need to perform the following operations. See *Updating the LDAP Schema* (on page 231) for information about updating the AD LDAP/LDAPS schema.

► **To enable your AD server on the KX II-101:**

1. Using the KX II-101, create special groups and assign proper permissions and privileges to these groups. For example, create groups such as KVM_Admin and KVM_Operator.
2. On your Active Directory server, create new groups with the same group names as in the previous step.
3. On your AD server, assign the KX II-101 users to the groups created in step 2.
4. From the KX II-101, enable and configure your AD server properly. See **Implementing LDAP/LDAPS Remote Authentication** (on page 127).


Important Notes:

- Group Name is case sensitive.
- The KX II-101 provides the following default groups that cannot be changed or deleted: Admin and <Unknown>. Verify that your Active Directory server does not use the same group names.
- If the group information returned from the Active Directory server does not match a KX II-101 group configuration, the KX II-101 automatically assigns the group of <Unknown> to users who authenticate successfully.

Implementing RADIUS Remote Authentication

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

► **To use the RADIUS authentication protocol:**

1. Click User Management > Authentication Settings to open the Authentication Settings page.
2. Click elect the RADIUS radio button to enable the RADIUS section of the page.
3. Click the  icon to expand the RADIUS section of the page.
4. In the Primary Radius Server and Secondary Radius Server fields, type the IP address of your primary and optional secondary remote authentication servers, respectively (up to 37 characters).
5. In the Shared Secret fields, type the server secret used for authentication (up to 37 characters).

The shared secret is a character string that must be known by both the KX II-101 and the RADIUS server to allow them to communicate securely. It is essentially a password.

6. The Authentication Port default is port is 1812 but can be changed as required.
7. The Accounting Port default port is 1813 but can be changed as required.
8. The Timeout is recorded in seconds and default timeout is 1 second, but can be changed as required.

The timeout is the length of time the KX II-101 waits for a response from the RADIUS server before sending another authentication request.

9. The default number of retries is 3 Retries.

This is the number of times the KX II-101 will send an authentication request to the RADIUS server.

10. Choose the Global Authentication Type from among the options in the drop-down list:
 - PAP - With PAP, passwords are sent as plain text. PAP is not interactive. The user name and password are sent as one data package once a connection is established, rather than the server sending a login prompt and waiting for a response.

- CHAP - With CHAP, authentication can be requested by the server at any time. CHAP provides more security than PAP.

Home > User Management > Authentication Settings

Authentication Settings

Local Authentication

LDAP

RADIUS

▶ LDAP

▼ RADIUS

Primary RADIUS Server

Shared Secret

Authentication Port
1812

Accounting Port
1813

Timeout (in seconds)
1

Retries
3

Secondary RADIUS Server

Shared Secret

Authentication Port
1812

Accounting Port
1813

Timeout (in seconds)
1

Retries
3

Global Authentication Type
PAP

OK Reset To Defaults Cancel

Returning User Group Information via RADIUS

When a RADIUS authentication attempt succeeds, the KX II-101 determines the permissions for a given user based on the permissions of the user's group.

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

RADIUS Communication Exchange Specifications

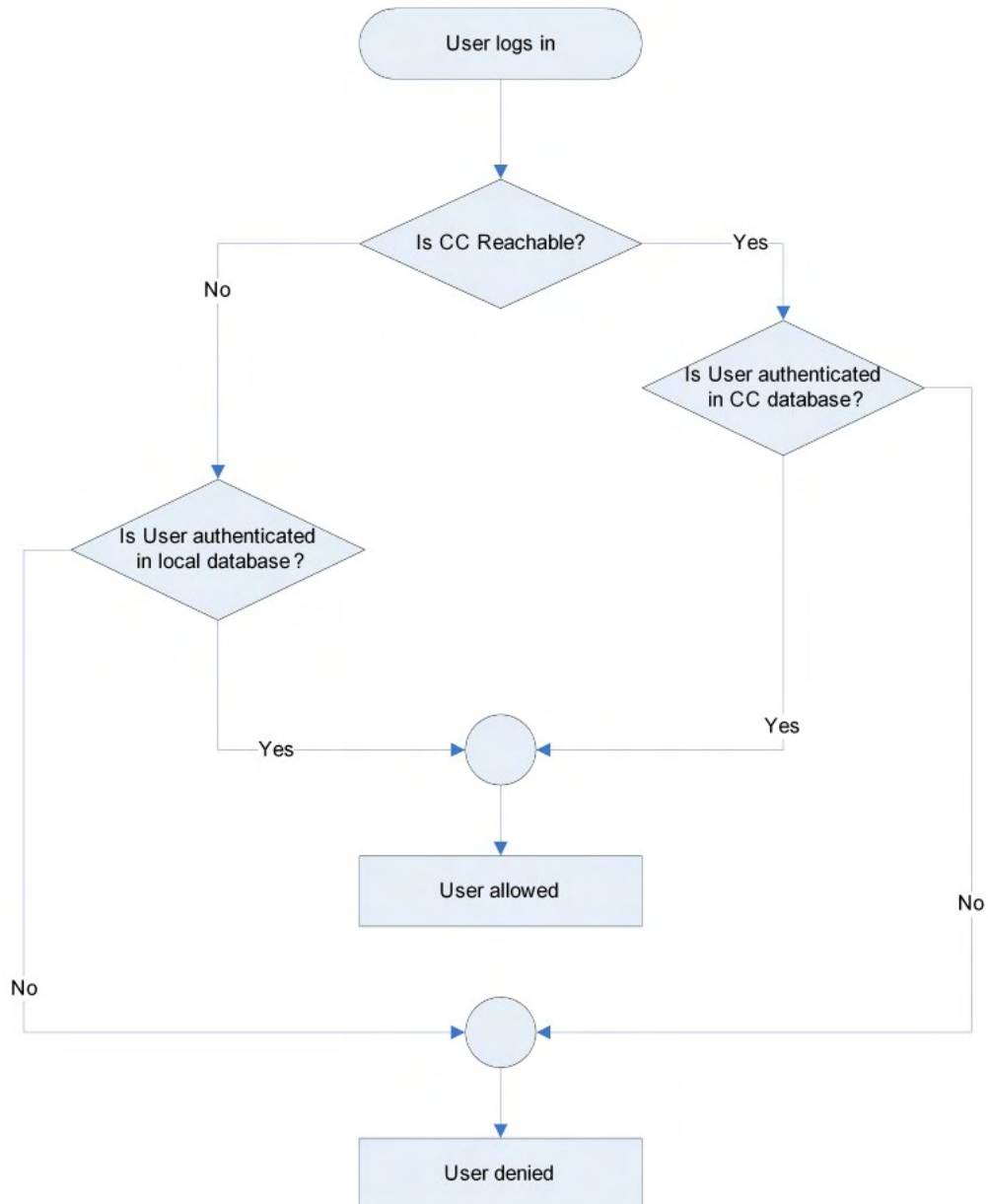
The KX II-101 sends the following RADIUS attributes to your RADIUS server:

Attribute	Data
Log on	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-IP-Address (4)	The IP address for the KX II-101.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
User-Password(2)	The encrypted password.
Accounting-Request(4)	
Acct-Status (40)	Start(1) - Starts the accounting.
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP address for the KX II-101.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
Log off	
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.

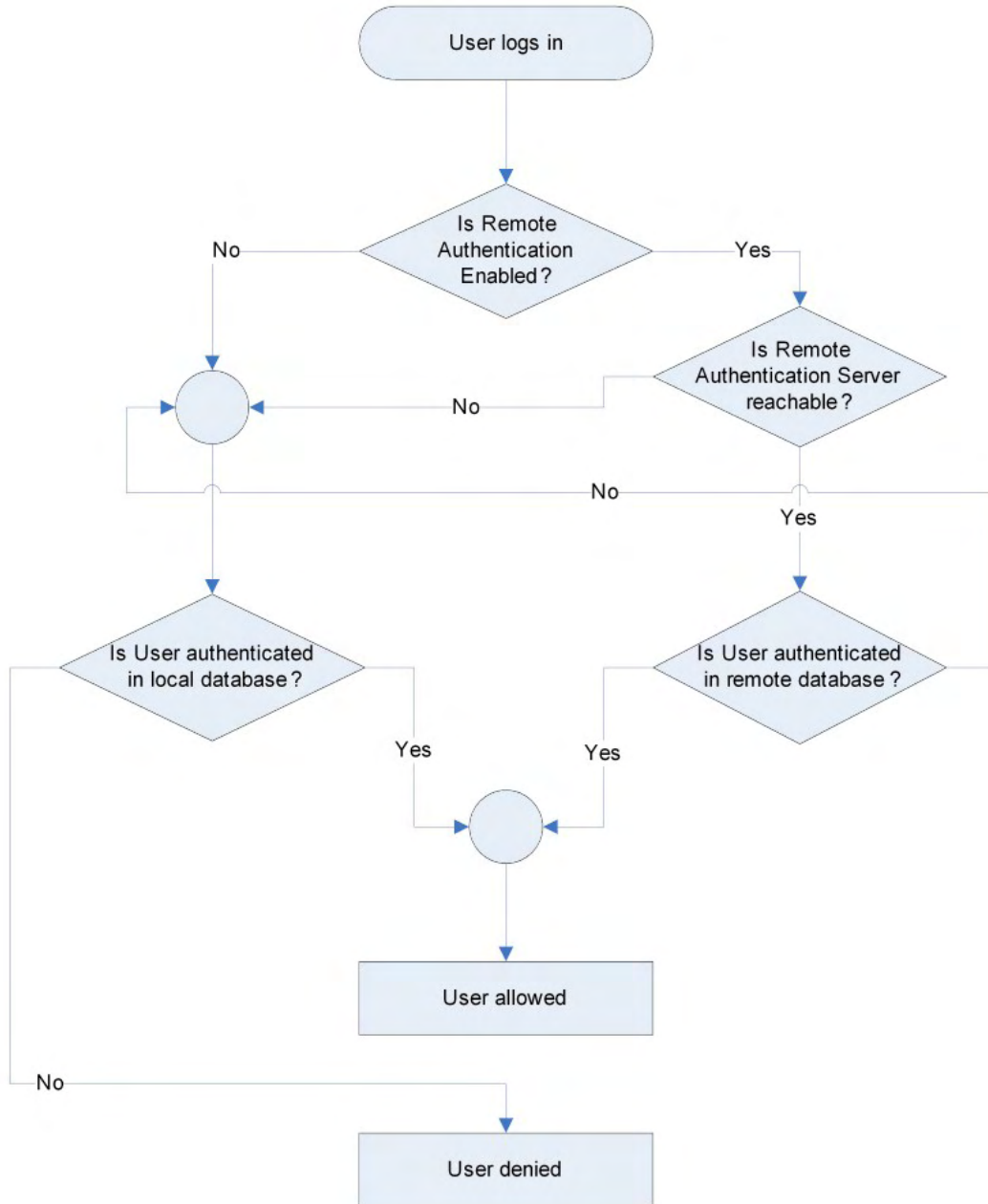
Attribute	Data
Log on	
NAS-IP-Address (4)	The IP address for the KX II-101.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

User Authentication Process

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:



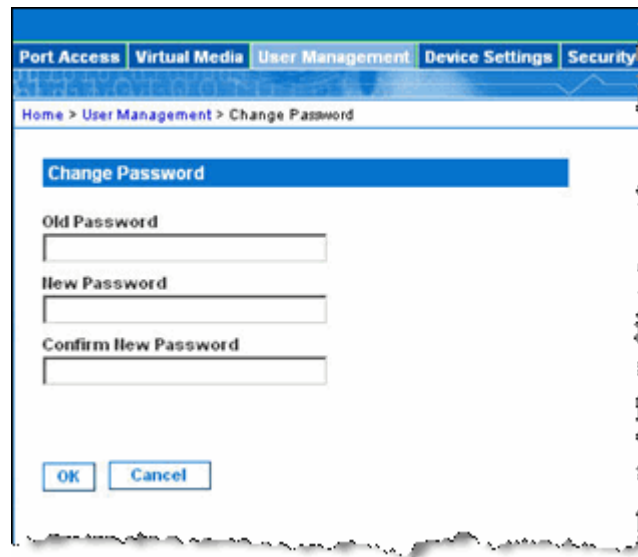
Remote authentication follows the process specified in the flowchart below:



Changing a Password

► **To change your password:**

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

The screenshot shows a web browser window with a navigation menu at the top containing 'Port Access', 'Virtual Media', 'User Management', 'Device Settings', and 'Security'. Below the menu is a breadcrumb trail: 'Home > User Management > Change Password'. The main content area has a blue header 'Change Password' and three text input fields labeled 'Old Password', 'New Password', and 'Confirm New Password'. At the bottom of the form are two buttons: 'OK' and 'Cancel'.

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

*Note: If strong passwords are in use, this page displays information about the format required for the passwords. For more information about passwords and strong passwords, see **Strong Passwords** (on page 186).*

Chapter 6 Device Management

In This Chapter

Network Settings	138
Device Services.....	141
Keyboard/Mouse Setup	143
Serial Port Settings.....	144
Date/Time Settings	148
Event Management	149
Port Configuration.....	154
Analog KVM Switch.....	162
Resetting the KX II-101 Using the Reset Button	163

Network Settings

Use the Network Settings page to customize the network configuration (for example, the IP address, discovery port, and LAN interface parameters) for your KX II-101.

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

- None (default) - This is the recommended option (static IP). Since the KX II-101 is part of your network infrastructure, you most likely do not want its IP address to change frequently. This option allows you to set the network parameters.
- DHCP - With this option, the IP address is automatically assigned by a DHCP server.

► **To change the network configuration:**

1. Choose Device Settings > Network. The Network Settings page opens.
2. Update the Network Basic Settings. See **Network Basic Settings** (on page 139).
3. Update the LAN Interface Settings. See **LAN Interface Settings** (on page 140).
4. Click OK to set these configurations. If your changes require rebooting the device, a reboot message appears.

► **To reset to factory defaults:**

- Click Reset to Defaults.

Network Basic Settings

1. Choose Device Settings > Network. The Network Settings page opens.
2. Specify a meaningful Device Name for your KX II-101 device using up to 16 alphanumeric characters, valid special characters, and no spaces.
3. In the IP Address section, enter or select the appropriate network settings:
 - a. Enter the IP Address if needed. The default IP address is 192.168.0.192.
 - b. Enter the Subnet Mask. The default subnet mask is 255.255.255.0.
 - c. Enter the Default Gateway if None is selected from the IP Auto Configuration drop-down.
 - d. Enter the Preferred DHCP Host Name if DHCP is selected from the IP Auto Configuration drop-down.

Note: The recommended host name length is 80 characters.

- e. Select the IP Auto Configuration. The following options are available:
 - None (Static IP) - This option requires that you manually specify the network parameters.

This is the recommended option because the KX II-101 is an infrastructure device and its IP address should not change.
 - DHCP - Dynamic Host Configuration Protocol is used by networked computers (clients) to obtain unique IP addresses and other parameters from a DHCP server.

With this option, network parameters are assigned by the DHCP server. If DHCP is used, enter the Preferred host name (DHCP only). Up to 80 characters.
4. Select Obtain DNS Server Address Automatically if DHCP is selected and Obtain DNS Server Address is enabled. When Obtain DNS Server Address Automatically, the DNS information provided by the DHCP server will be used.
5. If Use the Following DNS Server Addresses is selected, regardless of whether DHCP is selected, the addresses entered in this section will be used to connect to the DNS server.

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

 - a. Primary DNS Server IP Address
 - b. Secondary DNS Server IP Address
6. When finished, click OK. Your KX II-101 is now network accessible.

LAN Interface Settings

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

- Select the LAN Interface Speed & Duplex settings.
 - Autodetect (default option)
 - 10 Mbps/Half - Yellow LED blinks
 - 10 Mbps/Full - Yellow LED blinks
 - 100 Mbps/Half - Yellow LED blinks and the green LED is always lit
 - 100 Mbps/Full - Yellow LED blinks and the green LED is always lit

Half-duplex provides for communication in both directions, but only one direction at a time (not simultaneously).

Full-duplex allows communication in both directions simultaneously.

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

See **Network Speed Settings** (on page 228).

- Select the Bandwidth Limit.
 - No Limit
 - 128 Kilobit
 - 256 Kilobit
 - 512 Kilobit
 - 2 Megabit
 - 5 Megabit
 - 10 Megabit
 - 100 Megabit

Device Services

Use the Device Services page to specify the connection options for the KX II-101.

▶ To configure the discovery port:

1. Choose Device Settings > Device Services. The Device Services page opens.
2. Type the network port used by the KX II-101 to communicate with the Client PC.
3. Click Save to save the setting.

▶ To enable TELNET Access:

1. Choose Device Settings > Device Services. The Device Services page opens.
2. Select Enable TELNET Access.
3. Type the network port used for TELNET access to the KX II-101.
4. Click Save to save the setting.

▶ To enable SSH Access:

1. Choose Device Settings > Device Services. The Device Services page opens.

Note: KX II-101 is enabled by factory default.

2. Select Enable SSH Access.
3. Type the network port used for SSH access to the KX II-101.
4. Click Save to save the setting.

Enabling Direct Port Access

Direct port access enables you to access the KX II-101 Remote Client without having to go through the usual login page. With direct port access enabled, you can define a URL to navigate directly to the Port Access page.

▶ To enable direct port access:

1. Choose Device Settings > Device Services. The Device Services page opens.
2. Select the Enable Direct Port Access via URL checkbox.
3. Click Save to save the setting.

▶ To define a direct port access URL:

- Define a URL with the IP address, user name, password, and if necessary, port number of the KX II-101. If you have only one KVM port, the port number is not needed.

The format for a direct port access URL is:

`https://IP
address/dpa.asp?username=username&password=password&port=
port number`

Tip: Define a direct port access URL once, then save it in your web browser as a bookmark to make reusing it easier.

Home > Device Settings > Device Services

Services

Discovery Port *

5000

Enable TELNET Access

TELNET Port

23

Enable SSH Access

SSH Port

22

Enable Direct Port Access via URL

OK Reset To Defaults Cancel

Keyboard/Mouse Setup

Use the Keyboard/Mouse Setup page to configure the Keyboard and Mouse interface between the KX II-101 and the host device.

Home > Device Settings > Keyboard/Mouse Setup

Keyboard/Mouse Setup

Host Interface

USB

To use the *USB* and/or *PS/2* interface you need a correct cabling between the managed host and the managing device. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only then you will have no remote keyboard access during the boot process of the host. If USB and PS/2 are both connected and you selected *Auto* as host interface then the card will choose USB if available or otherwise falls back to PS/2.

OK Reset To Defaults Cancel

1. Click Device Settings > Keyboard/Mouse.
2. Select the Host Interface. This selection determines if the KX II-101 sends keyboard and mouse data through the PS/2 or USB connections.
 - Auto - With this setting, the KX II-101 will use a USB connection if available, otherwise it will default to the PS/2 connection.

- USB - Forces the KX II-101 to use the USB connection to send Keyboard and Mouse data to the host device.
- PS/2 - Forces the KX II-101 to use the PS/2 connection to send Keyboard and Mouse data to the host device.

*Note: If you are using a Raritan switch on the front-end with a KX II-101, you must set the Host Interface to PS/2 in order for the configuration to work properly. See **Analog KVM Switch** (on page 162).*

3. Click OK.

▶ **To reset to factory defaults:**

- Click Reset To Defaults.

Serial Port Settings

Use the Serial Port Settings page to configure how the KX II-101 employs its integrated serial port.

Admin Port

▶ **To configure the admin serial port:**

1. Choose Device Settings > Serial Port. The Serial Port Settings page appears.
2. Select the Admin Port radio button, if it is not already selected (this is the default factory setting).

Choose this option to connect to the KX II-101 directly from a client PC and access the Command Line Interface through a program such as Hyperterminal. See **Command Line Interface (CLI)** (on page 210).

3. In the Serial Settings section, configure the following fields:
 - Speed
 - Stop Bits
 - Data Bits
 - Handshake
 - Parity

4. Click OK.

Home > Device Settings > Serial Port Settings

Serial Port Settings

Admin Port
 Powerstrip Control
 Modem

Serial Settings:

Speed: 115200 Stop Bits: 1
Data bits: 8 Handshake: None
Parity: none

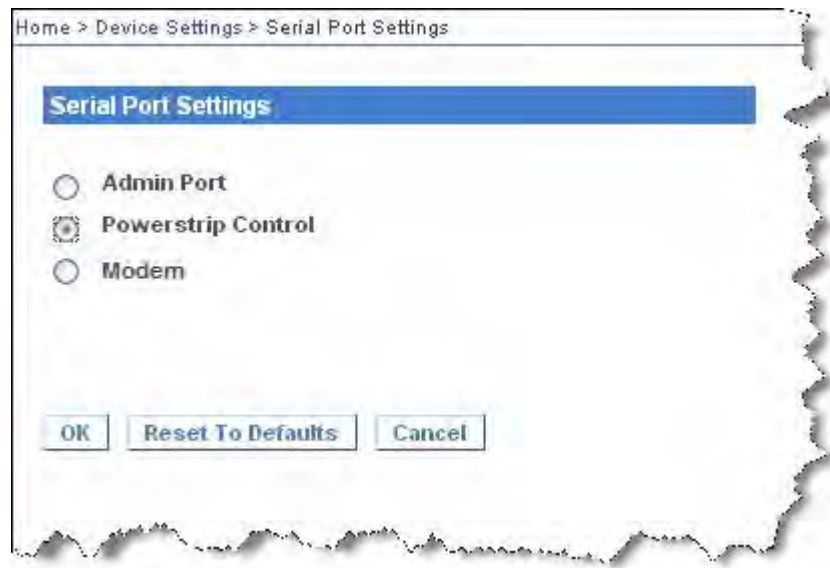
OK Reset To Defaults Cancel

Raritan Power Strip Control

► **To configure the power strip serial port:**

1. Choose Device Settings > Serial Port. The Serial Port Settings page opens.
2. Select the PowerStrip Control radio button. Choose this option when connecting the KX II-101 to a Raritan power strip.

3. Click OK.



Modem

► **To configure the modem serial port:**

1. Choose Device Settings > Serial Port. The Serial Port Settings page opens.
2. Select the Modem radio button. Choose this option when attaching an external modem to the KX II-101 in order to provide dial-up access.
3. In the Modem Settings section, configure the following fields:
 - Serial line speed
 - Modem init string - The default string displayed in the field must be used to enable modem access.
 - Modem server IP address - The address the user types to access the KX II-101 web interface once connected via modem.
 - Modem client IP address - The address assigned to the user once connected via modem.

4. Click OK.

Home > Device Settings > Serial Port Settings

Serial Port Settings

Admin Port
 Powerstrip Control
 Modem

Modem Settings:

Serial line speed
115200 bits/s

Modem init string
ATZHO OK ATL0M0&K3X1 OK

Modem server IP address
192.168.3.1

Modem client IP address
192.168.3.2

OK Reset To Defaults Cancel

See **Modem Access Cable Connections** (on page 148) for details on the cable connection for modem access and see **Certified Modems** (on page 226) for details on certified modems that work with the KX II-101. For information on settings that will give you the best performance when connecting to the KX II-101 via modem, see **Creating, Modifying and Deleting Profiles in MPC** (on page 74).

Modem Access Cable Connections

Use the following cable connection configuration to connect the KX II-101 to a modem:

1. Connect an admin serial cable to the KX II-101.
2. Connect a 9 pin male/male gender changer to the admin serial cable.
3. Connect a null modem cable to other side of the gender changer.
4. Connect the 9 pin male/male gender changer to other end of the null modem cable.
5. Connect a DB9 to male DB25 modem cable between the null modem cable and the modem.

Date/Time Settings

Use the Date/Time Settings page to specify the date and time for the KX II-101. There are two ways to do this:

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

► **To set the date and time:**

1. Choose Device Settings > Date/Time. The Date/Time Settings page opens.
2. Choose your time zone from the Time Zone drop-down list.
3. To adjust for daylight savings time, check the "Adjust for daylight savings time" checkbox.
4. 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.
For the User Specified Time option, enter the date and time. For the time, use the hh:mm format (using a 24-hour clock).
 - Synchronize with NTP Server - Choose this option to synchronize the date and time with the Network Time Protocol (NTP) Server.
5. For the Synchronize with NTP Server option:
 - a. Enter the IP address of the Primary Time server.
 - b. Enter the IP address of the Secondary Time server. **Optional**

6. Click OK.

Home > Device Settings > Date/Time Settings

Date/Time Settings

Time Zone
(GMT -05:00) US Eastern

Adjust for daylight savings time

User Specified Time

Date (Month, Day, Year)
May 09, 2008

Time (Hour, Minute)
10:18

Synchronize with NTP Server

Primary Time server
[Input Field]

Secondary Time server
[Input Field]

OK **Reset To Defaults** **Cancel**

Event Management

The KX II-101 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.

Configuring 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. The KX II-101 offers SNMP Agent support through Event Management.

► To configure SNMP (enable SNMP logging):

1. Choose Device Settings > Event Management - Settings. The Event Management - Settings page appears.
2. Select SNMP Logging Enabled. This enables the remaining SNMP fields.
3. In the Name, Contact, and Location fields, type the SNMP agent's name (that is, the device's name) as it appears in the KX II-101 Console interface, a contact name related to this device, and where the Dominion device is physically located.
4. Type the Agent Community String (the device's string). An SNMP community is the group to which devices and management stations running SNMP belong. It helps define where information is sent. The community name is used to identify the group. The SNMP device or agent may belong to more than one SNMP community.
5. 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/Host Name, 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.

► To configure the Syslog (enable Syslog forwarding):

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

► To reset to factory defaults:

- Click Reset To Defaults.

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 the system events to track and where to send this information.

*Note: SNMP traps will be generated only if the SNMP Logging Enabled option is selected. Syslog events will be generated only if the Enable Syslog Forwarding option is selected. Both of these options are in the Event Management - Settings page. See **Configuring Event Management - Settings** (on page 150).*

► To select events and their destinations:

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

Category	Event	SNMP	Syslog	Audit Log
Device Operation	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"/>
	Power Supply Status Changed	<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	Factory/Reset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Begin OC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	End OC 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"/>
	Device Update Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware Update Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware File Discarded	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware Validation Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Configuration Backed Up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Configuration Restored	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Security	Port Connection Denied	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Password Settings Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Login Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Password Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Activity	User Blocked	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Connected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Disconnected	<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. Select the checkboxes for those event line items you want to enable or disable, and where you want to send the information.

Tip: Enable or disable entire Categories by checking or clearing the Category checkboxes, respectively.

3. Click OK.

► **To reset to factory defaults:**

- Click Reset To Defaults.

Warning: When using SNMP traps over UDP, it is possible for the KX II-101 and the router that it is attached to to fall out of synchronization when the KX II-101 is rebooted, preventing the reboot completed SNMP trap from being logged.

SNMP Agent Configuration

SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP managers. Use the Event Logging page to configure the SNMP connection between the KX II-101 (SNMP Agent) and an SNMP manager.

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 KX II-101 SNMP traps:

Trap Name	Description
configBackup	The device configuration has been backed up.
configRestore	The device configuration has been restored.
deviceUpdateFailed	Device update has failed.
deviceUpgradeCompleted	The KX II-101 has completed update via an RFP file.
deviceUpgradeStarted	The KX II-101 has begun update via an RFP file.
factoryReset	The device has been reset to factory defaults.
firmwareFileDiscarded	Firmware file was discarded.
firmwareUpdateFailed	Firmware update failed.
firmwareValidationFailed	Firmware validation failed.
groupAdded	A group has been added to the KX II-101 system.
groupDeleted	A group has been deleted from the system.
groupModified	A group has been modified.
ipConflictDetected	An IP Address conflict was detected.

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 KX II-101 has completed its reboot.
rebootStarted	The KX II-101 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.
userAdded	A user has been added to the system.
userAuthenticationFailure	A user attempted to log in without a correct username and/or password.
userConnectionLost	A user with an active session has experienced an abnormal session termination.
userDeleted	A user account has been deleted.
userLogin	A user has successfully logged into the KX II-101 and has been authenticated.
userLogout	A user has successfully logged out of the KX II-101 properly.
userModified	A user account has been modified.

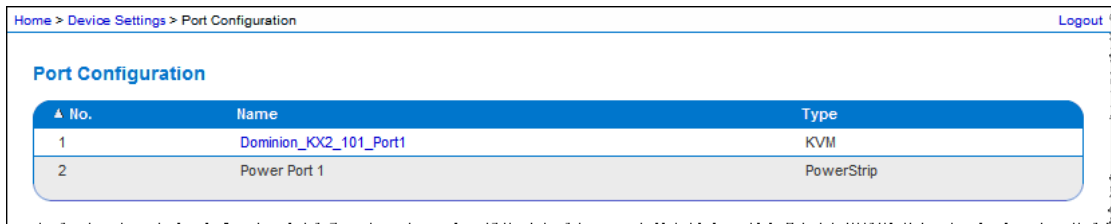
Trap Name	Description
userPasswordChanged	This event is triggered if the password of any user of the device is modified.
userSessionTimeout	A user with an active session has experienced a session termination due to timeout.
vmImageConnected	User attempted to mount either a device or image on the target 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

The Port Configuration page displays a list of the KX II-101 ports. Ports connected to KVM target servers or power strips are displayed in blue and can be edited.

► **To change a port configuration:**

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



Sorting

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 KX II-101 device.
- 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 Name.

- Port Type - The type of target connected to the port:

Port type	Description
PowerStrip	Power strip
KVM	KVM target

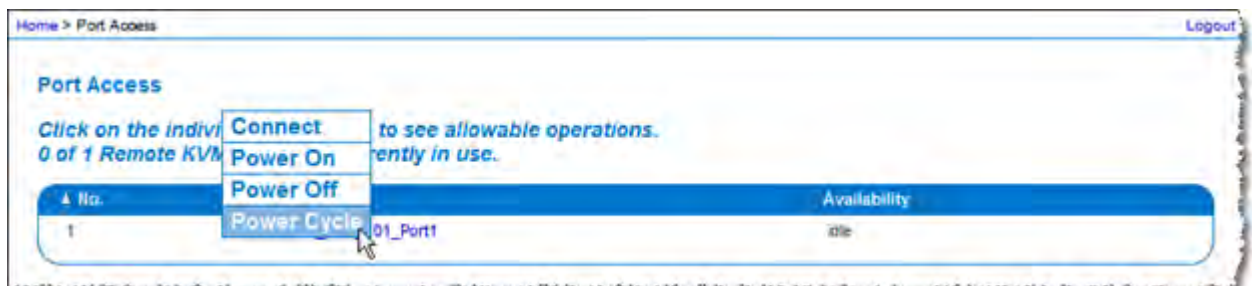
- Click the Port Name for the port you want to edit.
 - For KVM ports, the Port page is opened. In this page, you can name the ports, create power associations, and set target server settings.
 - For power strips, the Port page for power strips is opened. In this page, you can name the power strips and their outlets. See **Power Control** (on page 157).

Note: The Power Port 1 link is enabled only when a Raritan power strip is connected to the KX II-101 and configured. Otherwise, the link is disabled.

Managing KVM Target Servers (Port Page)

This Port page opens when you select a port from the Port Configuration page that is connected to a target server. From this page, you can make a power associations and change the Port Name to something more descriptive.

A server can have up to four power plugs that you can associate with the power strip. In this page, you can define those associations so that you can power on, power off, and power cycle the server from the Port Access page, as shown below.



*Note: To use this feature, you must have a Raritan Dominion PX power strip attached to the device. See **Connecting the Power Strip** (on page 157).*

► To access a port configuration:

- Choose Device Settings > Port Configuration. The Port Configuration page opens.
- Click the Port Name for the port you want to edit.

Note: The Power Port 1 link is enabled only when a Raritan power strip is connected to the KX II-101 and configured. Otherwise, the link is disabled.

Renaming a Port

► **To change the port name:**

1. Enter a descriptive name, such as the name of the target server. The name can be up to 32 alphanumeric characters and can include special characters.

Note: Do not use apostrophes for the Port Name.

2. Click OK.

Valid Special Characters

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

Power Control



The KX II-101 provides remote power control of a target server. To utilize this feature, you must have a Raritan remote power strip.

► To use the KX II-101 power control feature:

- Connect the power strip to your target server using the DKX2-101-SPDUC connector (not included but available from your reseller or Raritan). See **Connecting the Power Strip** (on page 157).
- Name the power strip (not included but available from your reseller or Raritan). See **Naming the Power Strip (Port Page for Power Strips)** (on page 158).
- Associate outlet in the power strip to the target server. See **Managing KVM Target Servers (Port Page)** (on page 155).
- Turn the outlets on the power strip on and off in the Power Strip Device page. See **Controlling a Power Strip Device** (on page 161).

Connecting the Power Strip



Diagram key	
	DKX2-101-SPDUC connector (not included) from the KX II-101 to Raritan the power strip.
	Raritan power strip.

► **To connect the KX II-101 to a Raritan power strip:**

1. Connect the Mini DIN9M connector of the DKX2-101-SPDUC cable to the Admin port of the KX II-101.
2. Connect the RJ45M connector of the DKX2-101-SPDUC cable to the serial port connector on the Raritan power strip.
3. Attach an AC power cord to the target server and an available power strip outlet on the power strip.
4. Connect the power strip to an AC power source.
5. Power ON the Raritan power strip.
6. Click to Device Settings > Serial Port to open the Serial Port page.
7. Select the Power Strip Control radio button and click OK. Once this is done, the Power menu is available on the Remote Console.

Naming the Power Strip (Port Page for Power Strips)

This Port page opens when you select a port, connected to a Raritan remote power strip, from the Port Configuration page. 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.

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).

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

Note: CommandCenter Service Gateway does not recognize power strip names containing spaces.

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 number.)

3. Click OK.

► **To cancel without saving changes:**

- Click Cancel.

Home > Device Settings > Port Configuration > Port

Port 2

Type:
PowerStrip

Name:
Power Port 1

Outlets

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

OK Cancel

© 2008 Raritan

Managing Power Associations

► **To make power associations (associate power strip outlets with the KVM target server):**

Note: When a power strip is associated with the target server (port), the outlet name is replaced by the port name. You can change this name in the Port 2 page.

1. Choose the power strip from the Power Strip Name drop-down list.
2. Choose the outlet from the Outlet Name drop-down list.
3. Repeat steps 1 and 2 for each desired power association.
4. Click OK. A confirmation message appears.

▶ **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 appears.

▶ **To show the power port configuration:**

- Choose Home > Device Settings > Port Configuration > [power port name]. The outlet associations for the power strip appear under Outlets.

▶ **To edit the power port configuration:**

1. Change the power port name by editing the port Name field.
2. Change an outlet name by editing the associated outlets Name field. The outlet name appears in the Power Strip Device page. See **Controlling a Power Strip Device** (on page 161).
3. Change the outlet association by clicking the Port Association link next to the outlet name and editing it in the Port 1 page.

Controlling a Power Strip Device

Control the power strip device using the Power Strip Device page. This page enables you to turn each outlet on the power strip on and off.

Home > Powerstrip

Powerstrip Device

Powerstrip: Power Port 1 - PCR8

Name:	Model:	Temperature:	CurrentAmps:	MaxAmps:	Voltage:	PowerInWatt:	PowerInVA:
Power Port 1	PCR8	41 °C	0.6 A	1.2 A	107 V	60 W	60 VA

Outlet 1: **off** (1)

Outlet 2: **off** (2)

Outlet 3: **off** (3)

Outlet 4: **off** (4)

Outlet 5: **off** (5)

Outlet 6: **off** (6)

Outlet 7: **on** (7)

Outlet 8: **on** (8)

► **To control the power strip connected to the KX II-101:**

1. Choose Home > Powerstrip. The Power Strip Device page opens.
2. Click the On or Off button for each outlet to run it on or off.
3. Click OK when prompted to confirm your choice.

Note: The KX II-101 can control only one power strip. You cannot select another power strip from the Powerstrip menu.

Analog KVM Switch

You can configure a Raritan analog KVM switch to work with the KX II-101.

The KX II-101's compatibility has been verified with the following Raritan KVM switches:

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

Similar products from Raritan or other vendors may be compatible but support is not guaranteed.

Note: In order for the KX II-101 to work with analog KVM switches, the switch hotkey that allows you to switch targets must be set to the Scroll Lock default.

► To configure a Raritan analog KVM switch:

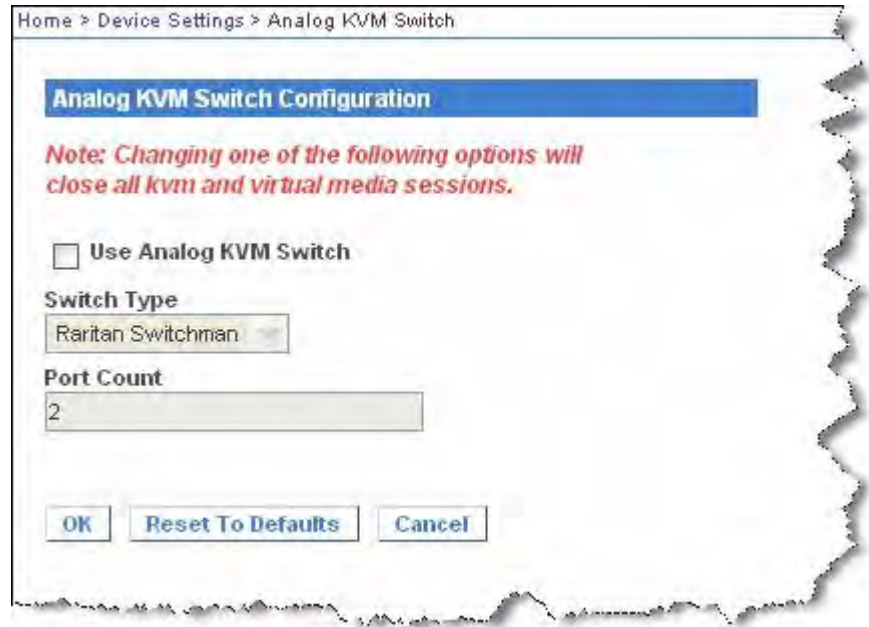
1. Set the Host Interface on the Keyboard/Mouse Setup page to PS/2. If you don't do this and try to configure an analog KVM switch, you will receive the error "PS/2 is needed to access the KVM Switch. Please enable PS/2 first!" on the Analog KVM Switch Configuration page. See **Keyboard/Mouse Setup** (on page 143).
2. Click Device Settings > Analog KVM Switch. The Analog KVM Switch Configuration page opens.
3. Select the Use Analog KVM Switch checkbox to enable to fields that you must define.
4. Select the Raritan switch type from the Switch Type drop-down:
 - Raritan MCC
 - Raritan MX
 - Raritan MXU
 - Raritan Switchman
5. The Port Count field will be populated with the number of ports available based on the switch type that is selected. Change the port count if needed or use the default counts. The defaults are:

Switch selection	Default port count
Raritan MCC	8
Raritan MX	16
Raritan MXU	16
Raritan Switchman	2

- Click OK to configure the analog KVM switch.

► **To restore analog KVM switch defaults:**

- Click Reset to Defaults.



Resetting the KX II-101 Using the Reset Button

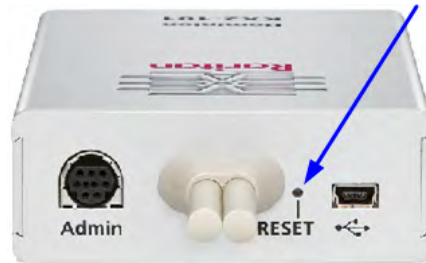
On the back panel of the KX II-101, there is a Reset button. It is recessed to prevent accidental resets (you will need a pointed object to press this button).

The actions that are performed when the Reset button is pressed are defined in the graphical user interface. See **Encryption & Share** (on page 190).

► **To reset the device:**

- Power off the KX II-101.
- Use a pointed object to press and hold the Reset button.
- While continuing to hold the Reset button, power the KX II-101 device back on.
- Continue holding the Reset button for 5-10 seconds.
- Release the Reset button and the KX II-101 will reboot. This typically takes three minutes.

NOTE: If the KX II-101 is set to restore to the factory defaults upon reset, the IP address, user name, and other options will be set accordingly.



Chapter 7 Managing USB Connections

In This Chapter

Overview	166
Basic USB Connection Settings	166
Advanced USB Connection Settings	168
Known USB Profiles	169

Overview

To broaden the KX II-101's compatibility with different KVM target servers, Raritan provides a user defined real-time selection of USB configuration profile options for a wide range of operating system and BIOS-level server implementations.

The default USB Connection Settings meets the needs of the vast majority of deployed KVM target server configurations. Additional configuration items are provided to meet the specific needs of other commonly deployed server configurations (for example, Linux and Mac OS X.. There are also a number of configuration items, designated by platform name and BIOS revision) to enhance virtual media function compatibility with the target server, for example, when operating at the BIOS level.

USB profiles are configured on the Device Settings > Port Configuration > Port page of the KX II-101 Remote Console. A device administrator can configure the port with the profiles that best meet the needs of the user and the target server configuration.

WARNING: It is possible, based on the selections you make in the Advanced USB Connection Settings section, to cause configuration problems between the KX II-101 and the target server.

Therefore, Raritan strongly recommends that you refer to the most recent User Defined KX II-101 USB Profile Configuration Table hyperlink, which can be accessed directly from the Advanced USB Connection Settings section on the Port page. The information available at the time of this publication can be found in **Known USB Profiles** (on page 169).

A user connecting to a KVM target server chooses among these USB Connection Settings depending on the operational state of the KVM target server. For example, if the server is running and the user wants to use the Windows operating system, it would be best to use the default settings. But if the user wants to change settings in the BIOS menu or boot from a virtual media drive, depending on the target server model, a different USB Connection Setting may be more appropriate.

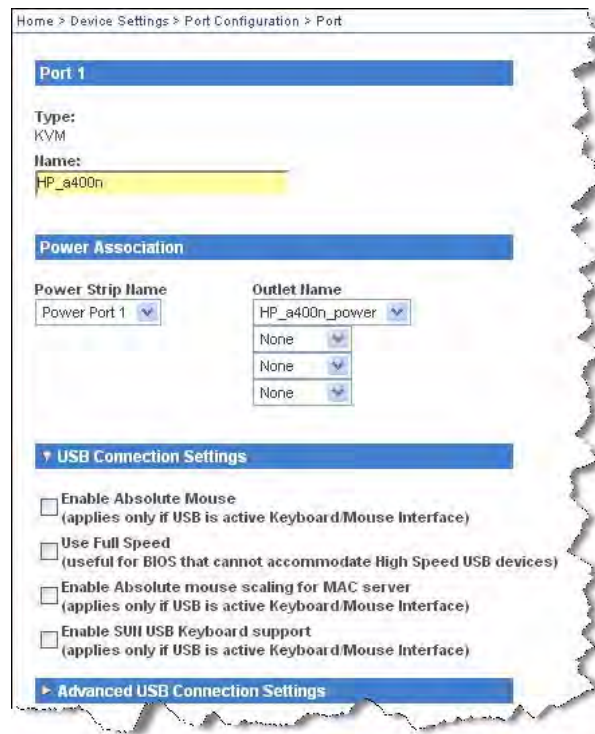
Should none of the USB Connection settings provided by Raritan work with a given KVM target, please contact Raritan Technical Support for assistance.

Basic USB Connection Settings

► **To define USB connections for the target server:**

1. Click Device Settings > Port Configuration to open the Port Configuration page. Click on the port you want to configure.


2. Click the **▶ USB Connection Settings** icon to expand the USB Connection Settings section.
3. Select the USB connection settings you will be using:
 - Enable Absolute Mouse - Applies only if USB is active Keyboard/Mouse Interface
 - Use Full Speed - Useful for BIOS that cannot accommodate High Speed USB devices
 - Enable Absolute mouse scaling for MAC server - Applies only if USB is active Keyboard/Mouse Interface
 - Enable SUN USB Keyboard support - Applies only if USB is active Keyboard/Mouse Interface
4. Click OK.



Advanced USB Connection Settings

WARNING: It is possible, based on the selections you make in the Advanced USB Connection Settings section, to cause configuration problems between the KX II-101 and the target server. Therefore, Raritan strongly recommends that you refer to the **Known USB Profiles** (on page 169) or to the User Defined KX II-101 USB Profiles Connection Configuration Table, which can be accessed by clicking its corresponding link on the Advanced USB Connection Settings section of the Port page .

► **To define advanced USB connections for the target server:**

1. Click Device Settings > Port Configuration to open the Port Configuration page. Click on the port you want to configure.
2. Click the  icon to expand the section.
3. Click the User Defined KX II-101 USB Profile Configuration Table link to access the recommended configurations to apply to the Advanced USB Connection Settings section.
4. Configure the following as needed:
 - Virtual Media Interface #1 Type
 - Check the Remove Unused VM Interface #1 From Device Configuration checkbox to remove the specified VM type interface (for #1).
 - Virtual Media Interface #2 Type
 - Check the Remove Unused VM Interface #2 From Device Configuration checkbox to remove the specified VM type interface (for #2).

5. Click OK.

Home > Device Settings > Port Configuration > Port

Port 1

Type:
KVM

Name:
HP_a400n

Power Association

Power Strip Name: Power Port 1

Outlet Name: HP_a400n_power

None

None

None

USB Connection Settings

Advanced USB Connection Settings

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

User Defined KX II-101 USB Profile Configuration Table

Virtual Media Interface #1 Type: CD-ROM

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

Virtual Media Interface #2 Type: Removable Disk

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

OK Cancel

Known USB Profiles

The current release of the KX II-101 includes the known USB profiles described in the following tables. However, for the most up-to-date USB profile information, please click on the User Defined KX II-101 USB Profiles Connection Configuration Table link in the Advanced USB Connection Settings section of the page.

Hardware/BIOS: Dell PowerEdge 1950/2950/2970/6950/R200

Server attributes:

BIOS v1.0.0, Windows Server 2003,
Intel Duo Core 800 MHz

Hardware/BIOS: Dell PowerEdge 1950/2950/2970/6950/R200			
Keyboard & mouse:		USB	
USB connection settings:		Advanced USB settings:	
Absolute mouse	<input checked="" type="checkbox"/>	Virtual media Intf#1	CD-ROM
Force full speed	<input type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	REM disk
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	
Comments: Standard configuration.			

Hardware/BIOS: Dell PowerEdge 1850			
Server attributes:		BIOS A06, Windows Server 2003, Intel Xeon 2.8GHz, provides support for USB Flash Emulation	
Keyboard & mouse:		PS/2	
USB connection settings:		Advanced USB settings:	
Absolute mouse	<input type="checkbox"/>	Virtual media Intf#1	CD-ROM
Force full speed	<input type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	REM disk
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	
Comments: Change the BIOS setup order to boot from an USB emulated device.			

Hardware/BIOS: Dell PowerEdge 650			
Server attributes:	BIOS A05, Windows Server 2003, Intel P 4 3GHz		
Keyboard & mouse:	USB		
USB connection settings:	Advanced USB settings:		
Absolute mouse	<input checked="" type="checkbox"/>	Virtual media Intf#1	CD-ROM
Force full speed	<input type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	REM disk
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	
Comments: BIOS accessible YES. No BIOS support to boot from USB emulated devices.			

Hardware/BIOS: Dell PowerEdge 1650	
Server attributes:	BIOS A11, Windows Server 2003, Intel P III 1.26GHz
Keyboard & mouse:	PS/2
USB connection settings:	Advanced USB settings:

Hardware/BIOS: Dell PowerEdge 1650			
Absolute mouse	<input type="checkbox"/>	Virtual media Intf#1	CD-ROM
Force full speed	<input checked="" type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	REM disk
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	

Comments: BIOS accessible YES. No BIOS support to boot from USB emulated devices.

Hardware/BIOS: Dell PowerEdge 2650			
Server attributes:		BIOS A21, Windows Server 2003, Intel Xeon 2.3 GHz	
Keyboard & mouse:		USB	
USB connection settings:		Advanced USB settings:	
Absolute mouse	<input checked="" type="checkbox"/>	Virtual media Intf#1	CD-ROM
Force full speed	<input checked="" type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	REM disk
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	

Comments: BIOS accessible YES. No BIOS support to boot from USB emulated devices.

Hardware/BIOS: Other Dell Optiplex, keyboard only			
Server attributes:		GX620 BIOS A11 11/20/06	
Keyboard & mouse:		USB	
USB connection settings:		Advanced USB settings:	
Absolute mouse	<input checked="" type="checkbox"/>	Virtual media Intf#1	Disabled
Force full speed	<input type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	Disabled
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	
Comments: BIOS keyboard access. Cannot boot from redirected drives (CD-ROM/USB)			

Hardware/BIOS: HP Compaq DC7100/7600			
Server attributes:		BIOS HP Pentium 4/mini tower	
Keyboard & mouse:		PS/2	
USB connection settings:		Advanced USB settings:	
Absolute mouse	<input checked="" type="checkbox"/>	Virtual media Intf#1	Auto
Force full speed	<input type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	Disabled
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	

Hardware/BIOS: HP Compaq DC7100/7600

Comments: Virtual CD-ROM and disk drives cannot be used simultaneously.

Hardware/BIOS: HP Integrity RX1600

Server attributes:		HP-UX 8.11 / CDE	
Keyboard & mouse:		USB	
USB connection settings:		Advanced USB settings:	
Absolute mouse	<input type="checkbox"/>	Virtual media Intf#1	CD-ROM
Force full speed	<input checked="" type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	REM disk
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	

Comments: Boot options accessible - YES. Intelligent Mouse mode, Standard Mouse mode, and Single Mouse mode are OK.

Hardware/BIOS: HP Proliant DL145

Server attributes:		PhoenixBIOS HP System BIOS-005 version 2.17, Build Date 9/26/06	
Keyboard & mouse:		PS/2	
USB connection settings:		Advanced USB settings:	

Hardware/BIOS: HP Proliant DL145			
Absolute mouse	<input type="checkbox"/>	Virtual media Intf#1	CD-ROM
Force full speed	<input checked="" type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	REM disk
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	
Comments: Boot from CD-ROM.			

Hardware/BIOS: HP Proliant DL145			
Server attributes:		PhoenixBIOS HP System BIOS-005 version 2.17, Build Date 9/26/06	
Keyboard & mouse:		PS/2	
USB connection settings:		Advanced USB settings:	
Absolute mouse	<input type="checkbox"/>	Virtual media Intf#1	Disable
Force full speed	<input checked="" type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	REM disk
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	
Comments: Boot from flash disk.			

Hardware/BIOS: HP Proliant DL360/DL380			
Server attributes:		HP Proliant DL360/DL380 G4 (HP SmartStart CD)	
Keyboard & mouse:		PS/2	
USB connection settings:		Advanced USB settings:	
Absolute mouse	<input type="checkbox"/>	Virtual media Intf#1	CD-ROM
Force full speed	<input checked="" type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	REM disk
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	
Comments: Use PS/2 keyboard/mouse for BIOS/SmartStart Installs.			

Hardware/BIOS: HP Proliant DL360/DL380	
Server attributes:	HP Proliant DL360/DL380 G4 (HP SmartStart CD)
Keyboard & mouse:	USB
USB connection settings:	Advanced USB settings:

Hardware/BIOS: HP Proliant DL360/DL380			
Absolute mouse	<input checked="" type="checkbox"/>	Virtual media Intf#1	CD-ROM
Force full speed	<input checked="" type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	REM disk
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	

Comments: Use USB keyboard/mouse and set the mouse to Absolute Mouse mode for normal desktop use.

Hardware/BIOS: HP Proliant DL360/DL380			
Server attributes:		HP Proliant DL360/DL380 G4 (Windows 2003 Server Installation)	
Keyboard & mouse:		PS/2	
USB connection settings:		Advanced USB settings:	
Absolute mouse	<input type="checkbox"/>	Virtual media Intf#1	CD-ROM
Force full speed	<input checked="" type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	REM disk
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	

Comments: Use PS/2 keyboard/mouse for BIOS/Windows Server 2003 installs.

Hardware/BIOS: HP Proliant DL360/DL380			
Server attributes:	HP Proliant DL360/DL380 G4 (Windows 2003 Server Installation)		
Keyboard & mouse:	USB		
USB connection settings:	Advanced USB settings:		
Absolute mouse	<input checked="" type="checkbox"/>	Virtual media Intf#1	CD-ROM
Force full speed	<input checked="" type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	REM disk
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	
Comments: Use USB keyboard/mouse and set the mouse to Absolute Mouse mode for normal desktop use.			

Hardware/BIOS: IBM eServer System P5	
Server attributes:	AIX Common Desktop Environment (CDE)
Keyboard & mouse:	USB
USB connection settings:	Advanced USB settings:

Hardware/BIOS: IBM eServer System P5			
Absolute mouse		Virtual media Intf#1	CD-ROM
Force full speed	✓	Remove Unused VM Intf#1	
Absolute mouse Mac server		Virtual Media Intf#2	REM disk
SUN USB keyboard		Remove Unused VM Intf#2	

Comments: Boot options accessible - YES. Only use Intelligent Mouse mode or Single Mouse mode.

Hardware/BIOS: IBM ThinkCentre Lenovo			
Server attributes:		BIOS Date 5-26-06, Intel P4 2.8 GHz	
Keyboard & mouse:		PS/2	
USB connection settings:		Advanced USB settings:	
Absolute mouse		Virtual media Intf#1	Auto
Force full speed		Remove Unused VM Intf#1	
Absolute mouse Mac server		Virtual Media Intf#2	Disabled
SUN USB keyboard		Remove Unused VM Intf#2	

Comments: ONLY redirected CD-ROM drives are supported. USB flash drives are not supported. Virtual CD-ROM and disk drives cannot be used simultaneously.

Hardware/BIOS: Lenovo ThinkPad X61			
Server attributes:		BIOS v1.11 2007-11-15 Intel Duo Core 2.20 GHz	
Keyboard & mouse:		USB	
USB connection settings:		Advanced USB settings:	
Absolute mouse	<input checked="" type="checkbox"/>	Virtual media Intf#1	Auto
Force full speed	<input checked="" type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input type="checkbox"/>	Virtual Media Intf#2	Disabled
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	
Comments: Press F1 during startup to enter BIOS. Press F12 to boot from the appropriate virtual media mount (CD-ROM/USB HDD).			

Hardware/BIOS: Lenovo ThinkPad T61	
Server attributes:	
BIOS v1.26 2007-10-18 Intel Core Duo 2.00GHz	
Keyboard & mouse:	
USB	
USB connection settings:	
Advanced USB settings:	

Hardware/BIOS: Lenovo ThinkPad T61

Absolute mouse	<input checked="" type="checkbox"/>	Virtual media Intf#1	Auto
Force full speed	<input checked="" type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server		Virtual Media Intf#2	Disabled
SUN USB keyboard		Remove Unused VM Intf#2	

Comments: Press F1 during startup to enter BIOS. Press F12 to boot from the appropriate virtual media mount (CD-ROM/USB HDD).

Hardware/BIOS: Mac

Server attributes:	BIOS Mac		
Keyboard & mouse:	USB		
USB connection settings:	Advanced USB settings:		
Absolute mouse		Virtual media Intf#1	CD-ROM
Force full speed		Remove Unused VM Intf#1	<input checked="" type="checkbox"/>
Absolute mouse Mac server		Virtual Media Intf#2	Disabled
SUN USB keyboard		Remove Unused VM Intf#2	

Comments: BIOS access setup. Virtual CD-ROM and disk drives cannot be used simultaneously.

Hardware/BIOS: Mac			
Server attributes:		BIOS Mac	
Keyboard & mouse:		USB	
USB connection settings:		Advanced USB settings:	
Absolute mouse	<input checked="" type="checkbox"/>	Virtual media Intf#1	CD-ROM
Force full speed	<input type="checkbox"/>	Remove Unused VM Intf#1	
Absolute mouse Mac server	<input checked="" type="checkbox"/>	Virtual Media Intf#2	Disabled
SUN USB keyboard	<input type="checkbox"/>	Remove Unused VM Intf#2	
Comments: Works normally on the Desktop. Virtual CD-ROM and disk drives cannot be used simultaneously.			

Hardware/BIOS: RUBY Industrial Mainboard (AwardBIOS)	
Server attributes:	RUBY Industrial Mainboard (AwardBIOS)
Keyboard & mouse:	PS/2
USB connection settings:	Advanced USB settings:

Hardware/BIOS: RUBY Industrial Mainboard (AwardBIOS)			
Absolute mouse		Virtual media Intf#1	Auto
Force full speed		Remove Unused VM Intf#1	
Absolute mouse Mac server		Virtual Media Intf#2	Disabled
SUN USB keyboard		Remove Unused VM Intf#2	

Comments: Use this for the RUBY-9715VG2A series industrial mainboards with Phoenix/AwardBIOS v6.00PG. Virtual CD-ROM and disk drives cannot be used simultaneously.

Chapter 8 Security Management

In This Chapter

Security Settings.....	184
Logon Limitations	185
Strong Passwords	186
User Blocking	188
Encryption & Share.....	190
Checking Your Browser for AES Encryption	192
IP Access Control	193

Security Settings

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

Raritan SSL certificates are used for public and private key exchanges, and provide an additional level of security. Raritan web server certificates are self-signed. Java applet certificates are signed by a VeriSign certificate. Encryption guarantees that your information is safe from eavesdropping and these certificates ensure that you can trust that the entity is Raritan, Inc.

► **To configure the security settings:**

1. Choose Security > Security Settings. The Security Settings page opens.
2. Update the **Logon Limitations** (on page 185) settings as appropriate.
3. Update the **Strong Passwords** (on page 186) settings as appropriate.
4. Update the **User Blocking** (on page 188) settings as appropriate.
5. Update the **Encryption & Share** (on page 190) settings as appropriate.
6. Click OK.

- ▶ **To reset back to defaults:**
 - Click Reset to Defaults.

Logon Limitations

Using logon limitations, you can specify restrictions for single logon, password aging, and the logging off of idle users.

Limitation	Description
Enable single logon limitation	When selected, only one login per user name is allowed at any time. When deselected, a given user name/password combination can be connected into the device from several client workstations simultaneously.

Limitation	Description
Enable password aging	<p>When selected, all users are required to change their passwords periodically based on the number of days specified in Password Aging Interval field.</p> <p>This field is enabled and required when the Enable Password Aging checkbox is selected. Enter the number of days after which a password change is required. The default is 60 days.</p>
Log off idle users	<p>When selected, the user session is automatically disconnected 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 off. If a virtual media session is in progress, however, the session does not timeout.</p> <p>The After field is used to set the amount of time (in minutes) after which an idle user will be logged off. This field is enabled when the Log Out Idle Users option is selected.</p>

Strong Passwords

Strong passwords provide more secure local authentication for the system. Using strong passwords, you can specify the format of valid KX II-101 local passwords such as minimum and maximum length, required characters, and password history retention.

Strong passwords

Enable strong passwords

Minimum length of strong password
8

Maximum length of strong password
16

Enforce at least one lower case character

Enforce at least one upper case character

Enforce at least one numeric character

Enforce at least one printable special character

Number of restricted passwords based on history
5

Strong passwords require user-created passwords to have a minimum of 8 characters with at least one alphabetical character and one nonalphabetical character (punctuation character or number). In addition, the first four characters of the password and the user name cannot match.

When selected, strong password rules are enforced. Users with passwords not meeting strong password criteria will automatically be required to change their password on their next login. When deselected, only the standard format validation is enforced. When selected, the following fields are enabled and required:

Field	Description
Minimum length of strong password	Passwords must be at least 8 characters long. The default is 8, but 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.
Enforce at least one printable special character	When checked, at least one special character (printable) is required in the password.
Number of restricted passwords based on history	This field represents the password history depth. That is, the number of prior passwords that cannot be repeated. The range is 1-12 and the default is 5.

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 screenshot shows a configuration window titled "User Blocking". It has three radio button options: "Disabled", "Timer Lockout", and "Deactivate User-ID". The "Deactivate User-ID" option is selected. Below the "Timer Lockout" option, there are two input fields: "Attempts" with the value "3" and "Lockout Time" with the value "5". Below the "Deactivate User-ID" option, there is one input field: "Failed Attempts" with the value "3".

The three options are mutually exclusive:

Option	Description
Disabled	The default option. Users are not blocked regardless of the number of times they fail authentication.

Option	Description
Timer Lockout	<p>Users are denied access to the system for the specified amount of time after exceeding the specified number of unsuccessful login attempts. When selected, the following fields are enabled:</p> <ul style="list-style-type: none"> ▪ Attempts - The number of unsuccessful login attempts after which the user will be locked out. The valid range is 1 - 10 and the default is 3 attempts. ▪ Lockout Time - The amount of time for which the user will be locked out. The valid range is 1 - 1440 minutes and the default is 5 minutes.
Deactivate User-ID	<p>When selected, this option specifies that the user will be locked out of the system after the number of failed login attempts specified in the Failed Attempts field:</p> <ul style="list-style-type: none"> ▪ Failed Attempts - The number of unsuccessful login attempts after which the user's User-ID will be deactivated. This field is enabled when the Deactivate User-ID option is selected. The valid range is 1 - 10.

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 KX II-101 Reset button is pressed.

WARNING: If you select an encryption mode that is not supported by your browser, you will not be able to access the KX II-101 from your browser.

Encryption & Share

Encryption Mode
 ▼

Apply Encryption Mode to KVM and Virtual Media

PC Share Mode
 ▼

VM Share Mode

Disable Local Port Output

Local Device Reset Mode
 ▼

1. Choose one of the options from the Encryption Mode drop-down list. When an encryption mode is selected, a warning appears, stating that if your browser does not support the selected mode, you will not be able to connect to the KX II-101. The warning states "When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the Dominion KX2-101."

Encryption mode	Description
Auto	This is the recommended option. The KX II-101 autonegotiates 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 that provides a private communications channel between the KX II-101 device and the Remote PC during initial connection authentication.

Encryption mode	Description
AES-128	The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data. 128 is the key length. When AES-128 is specified, be certain that your browser supports it, otherwise you will not be able to connect. See Checking Your Browser for AES Encryption (on page 192) for more information.
AES-256	The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data. 256 is the key length. When AES-256 is specified, be certain that your browser supports it, otherwise you will not be able to connect. See Checking Your Browser for AES Encryption (on page 192) for more information.

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

Note: If you are running Windows XP with Service Pack 2, Internet Explorer 7 cannot connect remotely to the KX II-101 using AES-128 encryption.

2. Apply Encryption Mode to KVM and Virtual Media. When selected, this option applies the selected encryption mode to both KVM and virtual media. After authentication, KVM and virtual media data is also transferred with 128-bit encryption.
3. PC Share Mode. Determines global concurrent remote KVM access, enabling up to eight remote users to simultaneously log into one KX II-101 and concurrently view and control the same target server through the device. Click the drop-down list to select one of the following options:
 - Private - No PC share. This is the default mode. Each target server can be accessed exclusively by only one user at a time.
 - PC-Share - KVM target servers can be accessed by up to eight users (administrator or non-administrator) at one time. Each remote user has equal keyboard and mouse control, however, note that uneven control will occur if one user does not stop typing or moving the mouse.
4. If needed, select VM Share Mode. This option is enabled only when PC-Share mode is enabled. When selected, this option permits the sharing of virtual media among multiple users, that is, several users can access the same virtual media session. The default is disabled.

5. If needed, select the Disable Local Port Output checkbox. If this option is selected, there is no video output on the local port.
6. If needed, select Local Device Reset Mode. This option specifies which actions are taken when the hardware Reset button (at the back of the device) is depressed. For more information, see **Resetting the KX II-101 - Using the Reset Button** (see "Resetting the KX II-101 Using the Reset Button" on page 163). Choose one of the following options:

PC Share mode	Description
Enable Local Factory Reset (default)	Returns the KX II-101 device to the factory defaults.
Enable Local Admin Password Reset	Resets the local administrator password only. The password is reset to raritan.
Disable All Local Resets	No reset action is taken.

Checking Your Browser for AES Encryption

The KX II-101 supports AES-256. If you do not know if your browser uses AES, check with the browser manufacturer or navigate to the <https://www.fortify.net/sslcheck.html> website using the browser with the encryption method you want to check. This website detects your browser's encryption method and displays a report.

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.x
- 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 link:

- JRE1.5 - http://java.sun.com/javase/downloads/index_jdk5.jsp

IP Access Control

Using IP access control, you can control access to your KX II-101. 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 KX II-101 as a whole, but you can also control access to your device at the group level.

Important: IP address 127.0.0.1 is used by the KX II-101 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 KX II-101 local port.

► **To use IP access control:**

1. Open the IP Access Control page by selecting Security > IP Access Control. 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 KX II-101 device.
 - Drop - IP addresses are denied access to the KX II-101 device.

► **To add (append) rules:**

1. Type the IP address and subnet mask in the IP/Mask field.

Note: The IP address should be entered using CIDR (Classless Inter-Domain Routing notation, in which the first 24 bits are used as a network address).

2. Choose the Policy from the drop-down list.
3. Click Append. The rule is added to the bottom of the rules list.

► **To insert a rule:**

1. Type a rule number (#). A rule number is required when using the Insert command.
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 number you just typed equals an existing rule number, the new rule is placed ahead of the existing rule and all rules are moved down in the list.

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

► **To replace a rule:**

1. Specify the rule number 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 number.

► **To delete a rule:**

1. Specify the rule number you want to delete.
2. Click Delete.
3. You are prompted to confirm the deletion. Click OK.

Home > Security > IP Access Control

IP Access Control

Enable IP Access Control

Default policy
ACCEPT

Rule #	IP Mask	Policy
		ACCEPT

Append Insert Replace Delete

OK Reset To Defaults Cancel

Chapter 9 Maintenance

In This Chapter

Audit Log.....	195
Device Information.....	196
Backup and Restore	197
Upgrading Firmware	198
Upgrade History.....	200
Rebooting	201

Audit Log

A log is created of the KX II-101 system events.

▶ **To view the audit log for your KX II-101:**

1. Choose Maintenance > Audit Log. The Audit Log page opens.

The Audit Log page displays events by date and time (most recent events listed first). The Audit Log provides the following information:

- Date - The date and time that the event occurred based on a 24-hour clock.
- Event - The event name as listed in the Event Management page.
- Description - Detailed description of the event.

▶ **To save the audit log:**

1. Click Save to File. A Save File dialog appears.
2. Choose the desired file name and location and click Save. The audit log is saved locally on your client machine with the name and location specified.

▶ **To page through the audit log:**

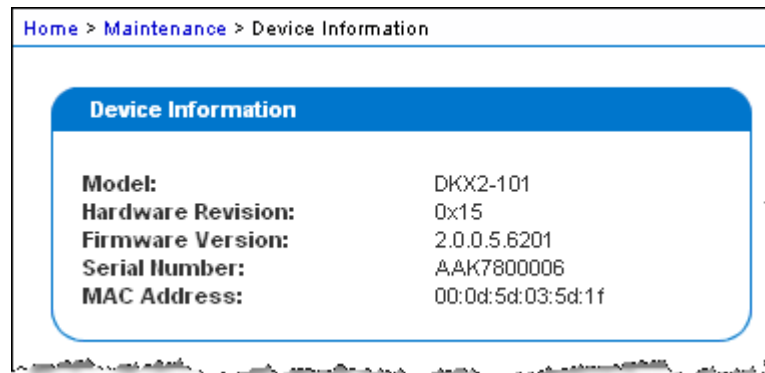
- Use the [Older] and [Newer] links.

Device Information

The Device Information page provides detailed information about your KX II-101 device. This information is helpful should you need to contact Raritan Technical Support.

► **To view information about your KX II-101:**

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



The following information is provided about the KX II-101:

- Model
- Hardware Revision
- Firmware Version
- Serial Number
- MAC Address

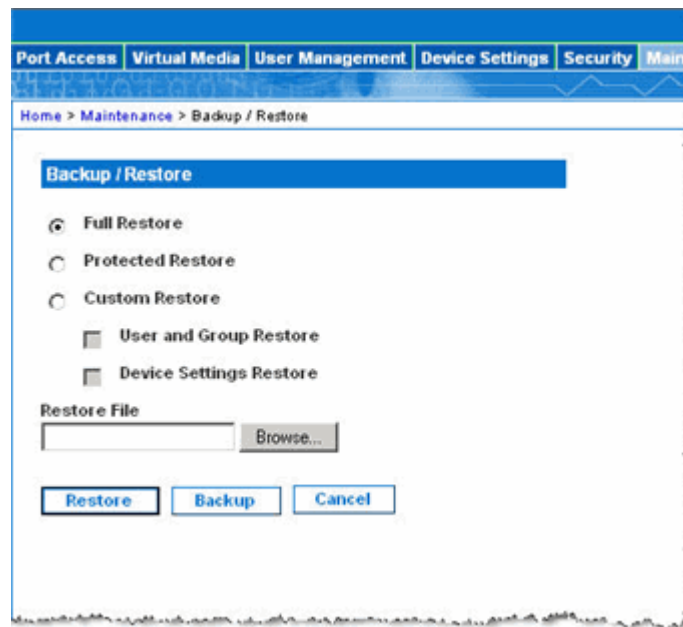
Backup and Restore

From the Backup/Restore page, you can backup and restore the settings and configuration for your KX II-101.

In addition to using backup and restore for business continuity purposes, you can use this feature as a time-saving mechanism. For instance, you can quickly provide access to your team from another KX II-101 by backing up the user configuration settings from the KX II-101 in use and restoring those configurations to the new KX II-101. You can also set up one KX II-101 and copy its configuration to multiple KX II-101 devices.

► To access the Backup/Restore page:

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



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

► To backup your KX II-101:

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

► **To restore your KX II-101:**

WARNING: Exercise caution when restoring your KX II-101 to an earlier version. Usernames and password in place at the time of the backup will be restored. If you do not remember the old administrative usernames and passwords, you will be locked out of the KX II-101.

In addition, if you used a different IP address at the time of the backup, that IP address will be restored as well. If the configuration uses DHCP, you may want to perform this operation only when you have access to the local port to check the IP address after the update.

1. Choose the type of restore you want to run:
 - Full Restore - A complete restore of the entire system. Generally used for traditional backup and restore purposes.
 - Protected Restore - Everything is restored except device-specific information such as IP address, name, and so forth. With this option, you can setup one KX II-101 and copy the configuration to multiple KX II-101 devices.
 - Custom Restore - With this option, you can select User and Group Restore, Device Settings Restore, or both. Select the appropriate checkboxes:
 - User and Group Restore - This option includes only user and group information. Use this option to quickly set up users on a different KX II-101.
 - Device Settings Restore - This option includes only device settings. Use this option to quickly copy the device information.
2. Click Browse. A Choose File dialog appears.
3. Navigate to and select the appropriate backup file and click Open. The selected file is listed in the Restore File field.
4. Click Restore. The configuration (based on the type of restore selected) is restored.

Upgrading Firmware

Use the Firmware Upgrade page to upgrade the firmware for your KX II-101.

Important: Do not turn off your KX II-101 device while the upgrade is in progress - doing so will likely result in damage to the device.

► **To upgrade your KX II-101 device:**

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

The screenshot shows a web interface titled "Firmware Upgrade". Below the title is a link "Show Latest Firmware". Underneath is a section labeled "Firmware File" containing a text input field and a "Browse..." button. At the bottom of this section are two buttons: "Upload" and "Cancel".

2. Click the Show Latest Firmware link, locate the appropriate Raritan firmware distribution file (*.RFP) from the Firmware Upgrades > KX II-101 page, and download the file.
3. Unzip the file and 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. Click the Browse button to navigate to the directory where you unzipped the upgrade file.

4. Click Upload from the Firmware Upgrade page. Information about the upgrade and version numbers is displayed for your confirmation:

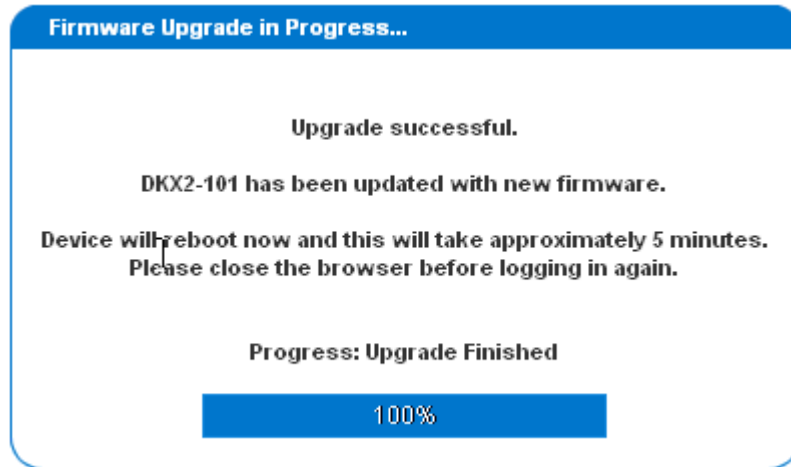
The screenshot shows the "Firmware Upgrade" page with a breadcrumb trail "Home > Maintenance > Firmware Upgrade". Below the title, it displays the following information:

Current version:	2.0.0.5.6394
New version:	2.0.0.5.6487

Below the table are two buttons: "Upgrade" and "Cancel". A warning message follows: "This may take some minutes. Please do NOT power off the device while the update is in progress! After a successful update, the device will be reset automatically."

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

- Click Upgrade. Wait for the upgrade to complete. Status information and progress bars are displayed during the upgrade. Upon completion of the upgrade, the device reboots.



- As prompted, close the browser and wait approximately 5 minutes before logging into the KX II-101 again.

For information about upgrading the device firmware using the Multi-Platform Client, see the **Raritan Multi-Platform Client (MPC) User Guide**.

Upgrade History

The KX II-101 provides information about upgrades performed on the KX II-101 device.

► **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	Result
Full Firmware Upgrade	admin	192.168.59.37	August 01, 2008 16:57	August 01, 2008 16:57	2.0.20.5.7034	2.0.20.5.7034	Successful
Full Firmware Upgrade	admin	192.168.59.37	August 01, 2008 16:19	August 01, 2008 16:22	2.0.20.5.7034	2.0.20.5.7034	Successful
Full Firmware Upgrade	admin	192.168.59.37	August 01, 2008 16:11	August 01, 2008 16:13	2.0.20.5.6955	2.0.20.5.7034	Successful
Full Firmware Upgrade	admin	192.168.59.37	August 01, 2008 16:09	August 01, 2008 16:09	2.0.20.5.6955	2.0.20.5.7034	Successful

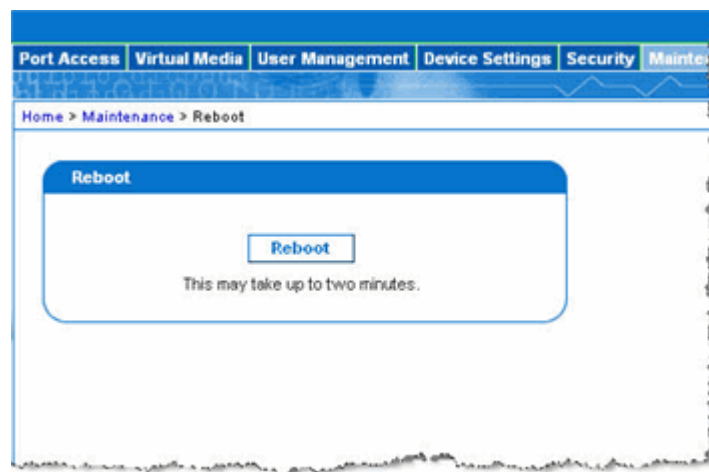
Rebooting

The Reboot page provides a safe and controlled way to reboot your KX II-101. This is the recommended method for rebooting.

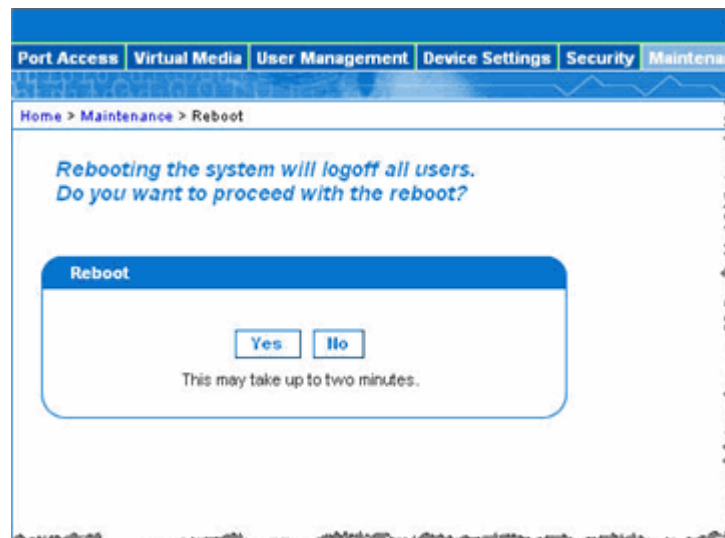
Important: All KVM and serial connections will be closed and all users will be logged off.

► **To reboot your KX II-101:**

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



2. Click Reboot. You are prompted to confirm the action. Click Yes to proceed with the reboot.



Chapter 10 Diagnostics

The Diagnostics pages are used for troubleshooting and are intended primarily for the administrator of the KX II-101 device. All of the Diagnostics pages (except Device Diagnostics) run standard networking commands and the information that is displayed is the output of those commands. The Diagnostics menu options help you debug and configure the network settings.

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

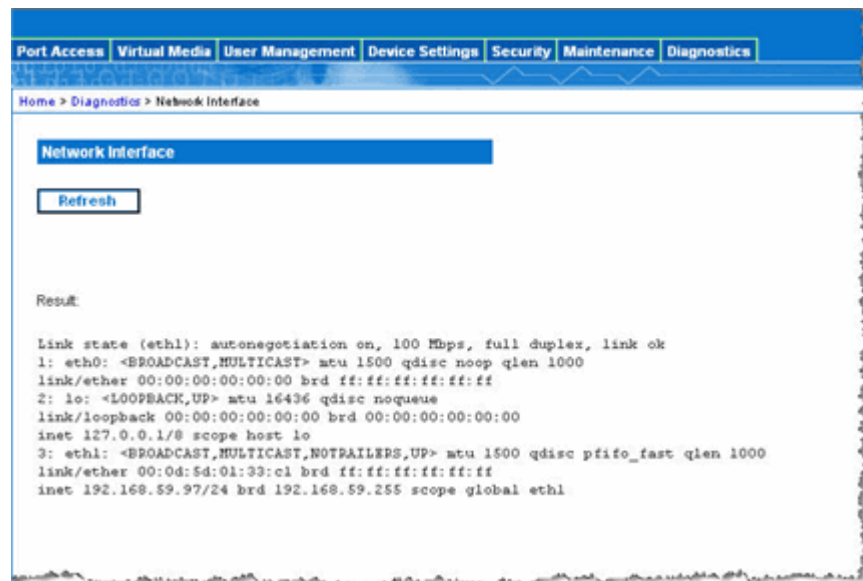
In This Chapter

Network Interface Page	202
Network Statistics Page.....	203
Ping Host Page.....	206
Trace Route to Host Page.....	206
Device Diagnostics	208

Network Interface Page

The KX II-101 provides information about the status of your network interface.

- ▶ **To view information about your network interface:**
 - Choose Diagnostics > Network Interface. The Network Interface page opens.



The following information is displayed:

- Whether the Ethernet interface is up or down.
- Whether the gateway is pingable or not.
- The LAN port that is currently active.

▶ **To refresh this information:**

- Click the Refresh button.

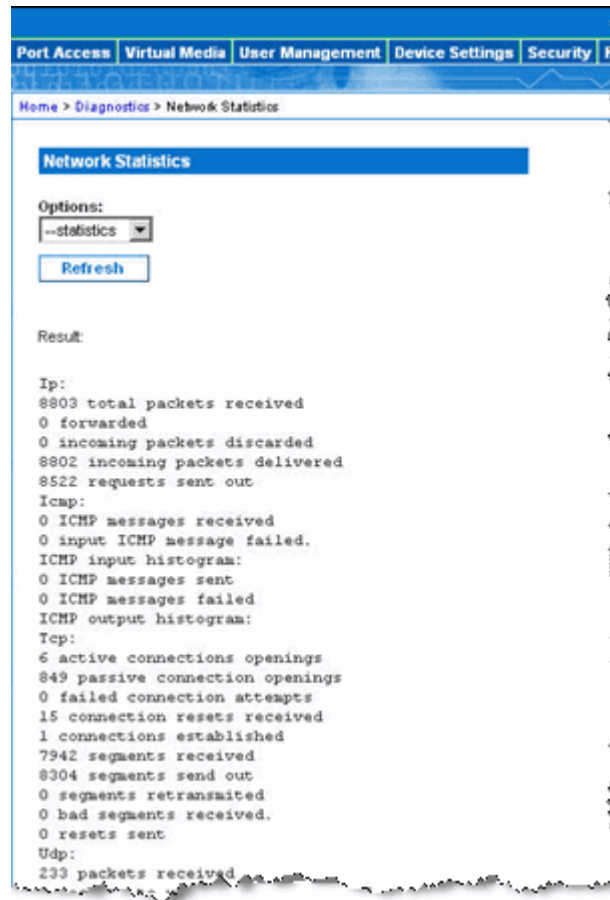
Network Statistics Page

The KX II-101 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.

The screenshot shows the 'Network Statistics' page in a web interface. The navigation bar includes 'Port Access', 'Virtual Media', 'User Management', 'Device Settings', 'Security', 'Maintenance', and 'Diagnostics'. The breadcrumb trail is 'Home > Diagnostics > Network Statistics'. The 'Options:' section has a dropdown menu set to '--interfaces' and a 'Refresh' button. The 'Result:' section displays the following text:

```
Kernel Interface table
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth1 1500 0 13828 0 0 0 8680 0 0 0 BMRU
lo 16436 0 196 0 0 0 196 0 0 0 LRU
```

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

The screenshot shows the 'Network Statistics' page in a web interface. The navigation bar includes 'Port Access', 'Virtual Media', 'User Management', 'Device Settings', 'Security', and 'Maint.'. The breadcrumb trail is 'Home > Diagnostics > Network Statistics'. The 'Options:' section has a dropdown menu set to '--route' and a 'Refresh' button. The 'Result:' section displays the following text:

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

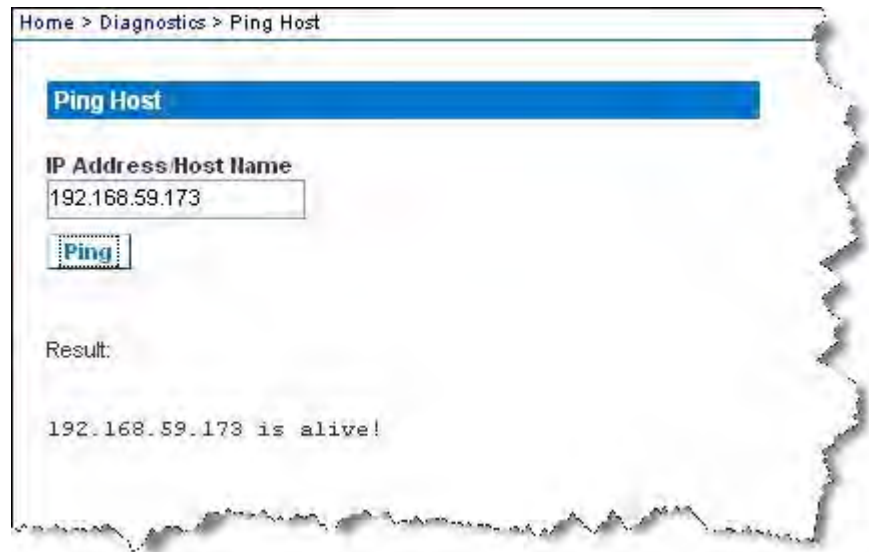
3. Click Refresh. The relevant information is displayed in the Result field.

Ping Host Page

Ping is a network tool used to test whether a particular host or IP address is reachable across an IP network. Using the Ping Host page, you can determine if a target server or another KX II-101 is accessible.

► **To ping the host:**

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



2. Type either the hostname or IP address into the IP Address/Host Name field.

Note: The host name cannot exceed 232 characters in length.

3. Click Ping. The results of the ping are displayed in the Result field.

Trace Route to Host Page

Trace route is a network tool used to determine the route taken to the provided hostname or IP address.

► **To trace the route to the host:**

1. Choose Diagnostics > Trace Route to Host. The Trace Route to Host page opens.
2. Type either the IP address or host name into the IP Address/Host Name field.

Note: The host name cannot exceed 232 characters in length.

3. Choose the maximum hops from the drop-down list (5 to 50 in increments of 5).
4. Click Trace Route. The trace route command is executed for the given hostname or IP address and the maximum hops. The output of trace route is displayed in the Result field.



Home > Diagnostics > Trace Route to Host

Trace Route to Host

IP Address: Host Name
192.168.59.173

Maximum Hops:
10

Trace Route

Result:

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

Device Diagnostics

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

The Device Diagnostics page downloads diagnostics information from the KX II-101 to the client machine. A device diagnostics log can be generated with or without running an optional diagnostic script provided by Raritan Technical Support. A diagnostics script produces more information for diagnosing problems.

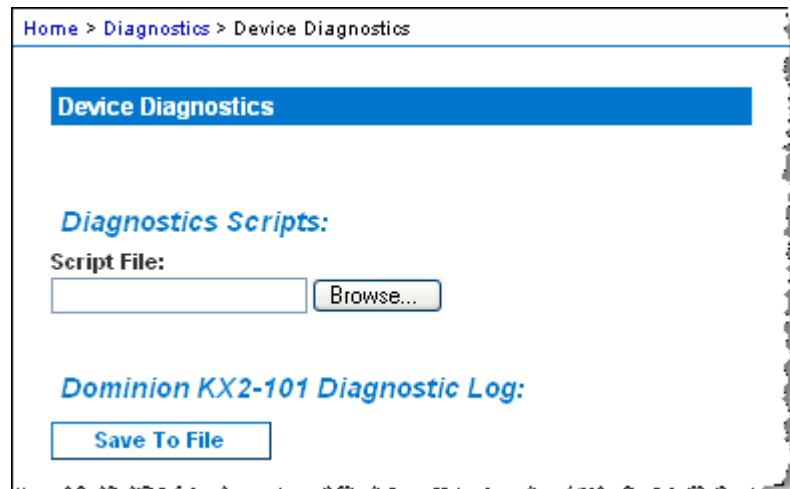
Use the following settings:

- Diagnostics Scripts - Loads a special script provided by Raritan Technical Support during a critical error debugging session. The script is uploaded to the device and executed. **Optional**
- Device Diagnostic Log - Downloads a snapshot of diagnostics messages from the KX II-101 device 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.

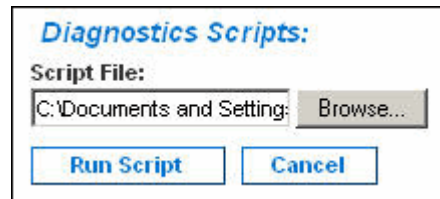
► **To run the KX II-101 System diagnostics:**

1. Choose Diagnostics > Device Diagnostics. The Device Diagnostics page opens.

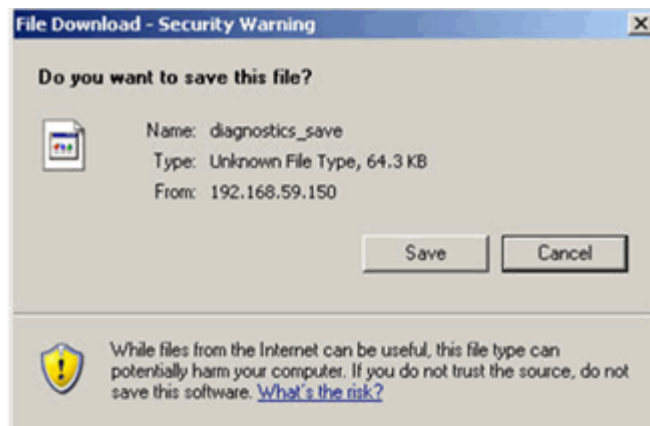


2. (Optional) Perform the following steps if you have received a diagnostics script file from Raritan Technical Support. Otherwise, skip to step 3.

- a. Retrieve the diagnostics file supplied by Raritan and unzip as necessary.
- b. Click Browse. A Choose File dialog appears.
- c. Navigate to and select this diagnostics file.
- d. Click Open. The file is displayed in the Script File field:



- e. Click Run Script.
3. Create a diagnostics file to send to Raritan Technical Support:
 - a. Click Save to File. The File Download dialog appears.



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

Chapter 11 Command Line Interface (CLI)

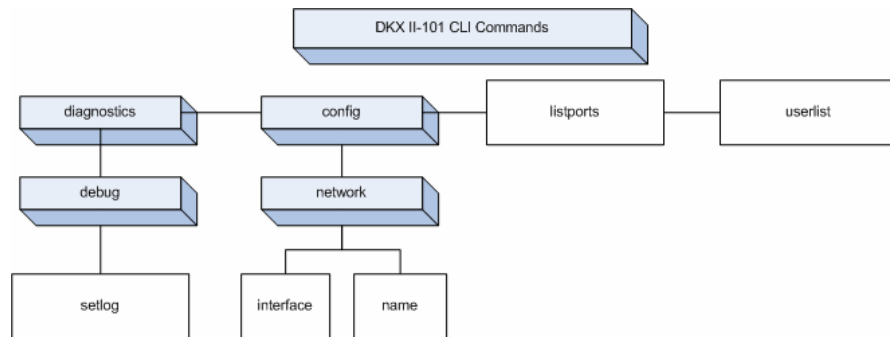
In This Chapter

Overview.....	210
Accessing the KX II-101 Using the CLI	211
SSH Connection to the KX II-101	211
Logging On	212
Navigation of the CLI.....	212
CLI Commands.....	214

Overview

This chapter provides an overview of the CLI commands that can be used with the KX II-101. See **CLI Commands** (on page 214) for a list of commands and definitions and links to the sections in this chapter that give examples of these commands.

The following diagram provides an overview of the CLI commands:



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

Accessing the KX II-101 Using the CLI

Access the KX II-101 using one of the following methods:

- TELNET via IP connection
- SSH (Secure Shell) via IP connection
- Multi-function admin serial port via RS-232 serial interface with provided cable and a terminal emulation program like HyperTerminal

Several SSH/TELNET clients are available and can be obtained from the following locations:

- PuTTY - <http://www.chiark.greenend.org.uk/~sgtatham/putty/>
<http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- SSH Client from ssh.com - www.ssh.com <http://www.ssh.com>
- Applet SSH Client - www.netspace.org/ssh
<http://www.netspace.org/ssh>
- OpenSSH Client - www.openssh.org <http://www.openssh.org>

*Note: Accessing the CLI by SSH or TELNET requires you to set up access in the Device Services page of the KX II-101 Remote Client. See **Device Services** (on page 141).*

SSH Connection to the KX II-101

Use any SSH client that supports SSHv2 to connect to the device. You must enable SSH access from the Devices Services page. See **Device Services** (on page 141).

Note: For security reasons, SSH V1 connections are not supported by the KX II-101.

SSH Access from a Windows PC

► **To open an SSH session from a Windows PC:**

1. Launch the SSH client software.
2. Enter the IP address of the KX II-101 server. For example, 192.168.0.192.
3. Choose SSH, which uses the default configuration port 22.
4. Click Open.
5. The login as: prompt appears.

See **Logging On** (on page 212).

SSH Access from a UNIX/Linux Workstation

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

```
ssh -l admin 192.168.30.222
```

The Password prompt appears.

See **Logging On** (on page 212).

Logging On

- ▶ To log in, enter the user name admin as shown:

1. Login: admin
2. The password prompt appears. Enter the default password: *raritan*.

The welcome message appears. You are now logged in as an Administrator.

```
Login: admin
Password:

-----
Device Type: Dominion KX2-101      Model: DKX2-101
Device Name: DKX2-101-DOC         FW Version: 2.0.0.5.6394      SN: AAK7800010
IP Address: 192.168.50.153        Idle Timeout: 30min
-----

Port Port          Port Port  Port
No.  Name            Type Status Availability
1 - Dominion_KXII-101_Port KUM up      idle

Current Time: Wed Dec 26 14:37:00 2007
Admin Port > _
```

After reviewing the following **Navigation of the CLI** (on page 212) section, you can perform the initial configuration tasks described in **Configure the KX II-101 Using a Terminal Emulation Program (Optional)** (on page 29).

Navigation of the CLI

Before using the CLI, it is important to understand CLI navigation and syntax. There are also some keystroke combinations that simplify CLI use.

CLI Prompts

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

```
admin >
```

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

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

Completion of Commands

The CLI supports the completion of partially-entered commands. After entering the first few characters of an entry, press the Tab key. If the characters form a unique match, the CLI will complete the entry.

- If no match is found, the CLI displays the valid entries for that level.
- If multiple matches are found, the CLI displays all valid entries.

Enter additional text to make the entry unique and press the Tab key to complete the entry.

CLI Syntax -Tips and Shortcuts

Tips

- Commands are listed in alphabetical order.
- Commands are not case sensitive.
- Parameter names are single word without underscore.
- Commands without arguments default to show current settings for the command.
- Typing a question mark (?) after a command produces help for that command.
- A pipe symbol (|) indicates a choice within an optional or required set of keywords or arguments.

Shortcuts

- Press the Up arrow key to display the last entry.
- Press Backspace to delete the last character typed.
- Press Ctrl + C to terminate a command or cancel a command if you typed the wrong parameters.
- Press Enter to execute the command.
- Press Tab to complete a command. For example, `Admin Port > Conf.` The system then displays the `Admin Port > Config > prompt.S`

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 KX II-101 CLI.
help	Display an overview of the CLI syntax.
quit	Places the user back one level.
logout	Logs out the user session.

CLI Commands

The table below lists and describes all available CLI commands.

Command	Description
config	Switch to the Configuration menu.
diagnostics (on page 215)	Switch to the diagnostics menu.
debug (on page 216)	Switch to debug menu.
help	Display an overview of the CLI syntax.
history	Display the current session's command line history.
interface	Configure the KX II-101 network interface.
listports (see "Listports Command" on page 218)	Lists the port, port name, port type, port status, and port availability.
logout	Logout of the current CLI session.
name (see "Name Command" on page 217)	Sets the device name.
network (on page 217)	Displays network configuration and enables you to configure network settings.
quit	Return to previous command.
setlog (see "Setlog Command" on page 216)	Sets device logging options.
top	Return to the root menu.
userlist (see "Userlist Command" on page 218)	Lists the number of active users, user names, port, and status.

Diagnostics

The Diagnostics menu enables you to set the logging options for different modules of the KX II-101. You should set logging options only when instructed by a Raritan Technical Support engineer. These logging options enable a support engineer to get the right kind of information for debugging and troubleshooting purposes. When instructed by a support engineer, you will be told how to set logging options and how to generate a log file to send to Raritan technical support.

Important: Set logging options only under the supervision of a Raritan Technical Support engineer.

Debug

The Diagnostics > Debug menu enables you to choose the Setlog command to set logging options for the KX II-101.

Setlog Command

The Setlog command enables you set the logging level for different modules of the KX II-101 and to view the current logging levels for each module. The syntax for the setlog command is:

```
setlog [module <module>] [level <level>] [vflag <vflag>]
[verbose <on|off>]

Set/Get diag log level
```

The Setlog command options are described in the following table. Raritan Technical Support will tell you how to configure these settings.

Command Option	Description
module	The module name.
level	The diagnostics level: <ul style="list-style-type: none"> ▪ err ▪ warn ▪ info ▪ debug ▪ trace
vflag	The type of verbose flag: <ul style="list-style-type: none"> ▪ timestamp ▪ module ▪ thread ▪ fileline
verbose [on off]	Turns verbose logging on and off.

Setlog Command Example

The following Setlog command sets the logging level to debug with verbose logging on for the libpp_serial module.

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

Configuration

The Configuration menu enables you to access the network commands used to configure the network interface and set the device name.

Network

The Configuration > Network commands are used to configure the KX II-101 network connection and device name.

Command	Description
interface	Configure the KX II-101 device network interface.
name	Set the device name.

Name Command

The name command is used to configure the device and host name.

Syntax

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

name Command Example

The following command sets the device name:

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

Interface Command

The interface command is used to configure the KX II-101 network interface. When the command is accepted, the device will drop the HTTP/HTTPS connection and initialize a new network connection. All HTTP/HTTPS users must reconnect to the device using the new IP address and the correct username and password. See **Installation and Configuration** (on page 9).

The syntax of the interface command is:

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

The network command options are described in the following table.

Command Option	Description
ipauto	Static or dynamic IP address
ip ipaddress	IP address of the KX II-101 assigned for access from the IP network
mask subnetmask	Subnet mask obtained from the IP administrator

Command Option	Description
gw ipaddress	Gateway IP address obtained from the IP administrator
mode <auto 100fdx>	Set Ethernet Mode to auto detect or force 100MB/s full duplex (100fdx)

Interface Command Example

The following command sets the IP address, mask, and gateway addresses, and sets the mode to auto detect.

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

Listports Command

The Listports command lists the number of active users, user names, port, and status.

Listports Command Example

```
Admin Port > listports

Port Port                Port Port  Port
No.  Name                  Type Status Availability
1 - Dominion_KXII-101_Port KVM  up      idle
```

Userlist Command

The Userlist command lists the port, port name, port type, port status, and port availability.

Userlist Command Example

```
Admin Port > Userlist

Active user number: 1

User Name | From          | Status
-----|-----|-----
admin    | Admin Port    | active
```

Chapter 12 CC Unmanage

In This Chapter

Overview.....	219
Removing a KX II-101 from CC-SG Management	220
Using CC-SG in Proxy Mode.....	221

Overview

When a KX II-101 device is under CommandCenter Secure Gateway control and you attempt to access the device directly using the KX II-101 Remote Console, the following message appears (after entry of a valid user name and password).

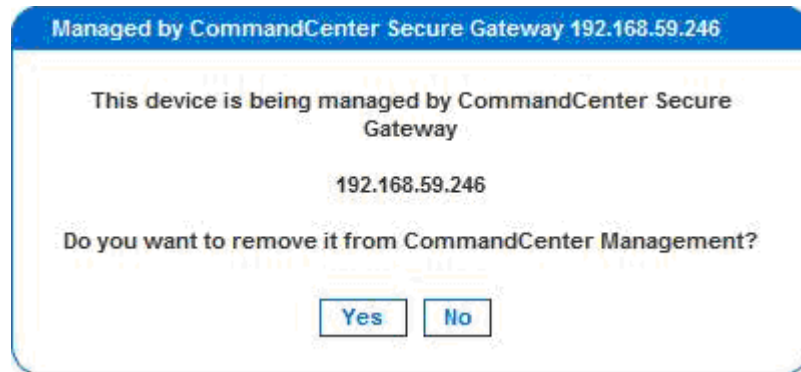


Removing a KX II-101 from CC-SG Management

Unless the KX II-101 is released from CC-SG control, you cannot access the device directly. However, if the KX II-101 does not receive heartbeat messages from CommandCenter (for example, CommandCenter is not on the network), you can release the KX II-101 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 appears when attempting to access the device directly.

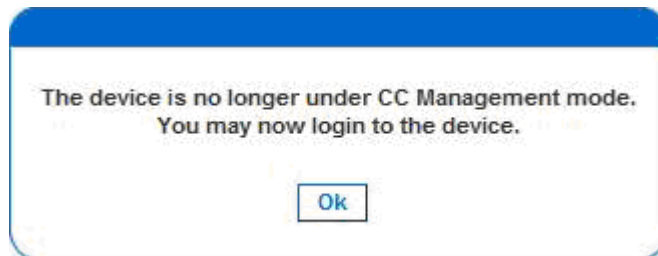


► **To remove the device from CC-SG management (to use CC Unmanage):**

1. Click Yes. You are prompted to confirm the action.



2. Click Yes. A message appears, confirming that the device is no longer under CC management.



3. Click OK. The KX II-101 login page opens.

Using CC-SG in Proxy Mode

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 the KX II-101 in a CC-SG configuration, do not use the CC-SG proxy mode if you are planning to use the Multi-Platform Client (MPC).

Appendix A Specifications

In This Chapter

KX II-101 Specifications	222
Supported Video Resolutions	223
Supported Keyboard Languages	224
Supported Operating Systems (Clients)	225
Supported Browsers	225
Certified Modems	226
Connectors	226
TCP and UDP Ports Used	226
Network Speed Settings	228
Admin Port Pinout Information	229
9 Pin Pinout	230

KX II-101 Specifications

Specification	Description
Form factor	Zero U form factor. Vertically or horizontally rack mountable (bracket kit included).
Dimensions (DxWxH)	4.055"x 2.913"x 1.063"; 103 x 74 x 27mm
Weight	0.6292lbs; 0.286kg
Power	<ul style="list-style-type: none"> • AC/DC (100-240V~/ 6VDC) • Power over Ethernet (PoE) <ul style="list-style-type: none"> ▪ Mid-Span Power Insertion ▪ Signal-Pair Power Insertion
Operating temperature	0° - 40°C (32° - 104°F)
Humidity	20% - 85% RH
Indicators: <ul style="list-style-type: none"> • Blue RARITAN back-lit logo • Network Port 	<ul style="list-style-type: none"> • Boot-up and power-level indicator • Network activity and connection speed indicator
Local connection	<ul style="list-style-type: none"> • 1- Mini USB port for USB keyboard / mouse and virtual media connectivity to the target • 1- MiniDIN9 port for multi-function serial port of full RS-232 features, modem connection, and Dominion PX connectivity

Specification	Description
Remote connection: <ul style="list-style-type: none"> Network Protocols 	<ul style="list-style-type: none"> One 10/100 Ethernet (RJ45) port TCP/IP, HTTP, HTTPS, UDP, RADIUS, LDAP, SNMP, DHCP
Screen resolutions: <ul style="list-style-type: none"> PC graphic mode SUN® video mode 	<ul style="list-style-type: none"> 720x400 (for DOS) 640 X 480 @ 60/72/75/85Hz, 800 X 600 @ 56/60/72/75/85Hz, 1024 X 768 @ 60/70/75/85Hz, 1152 X 864 @ 60/75Hz, 1280 X 1024 @ 60Hz, 1600 X 1200 @ 60Hz
Certifications	sUL/CUL, FCC Class A, CB, CE Class A and VCCI Class A

Supported Video Resolutions

Ensure that each target server's video resolution and refresh rate are supported by the KX II-101 and that the signal is noninterlaced.

The KX II-101 supports these resolutions:

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

Resolutions		
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.

Supported Keyboard Languages

The KX II-101 provides keyboard support for the languages listed in the following table.

Language	Regions	Keyboard layout
US English	United States of America and most of English-speaking countries: for example, Canada, Australia, and New Zealand.	US Keyboard layout
US English International	United States of America and most of English-speaking countries: for example, Netherlands	US Keyboard layout
UK English	United Kingdom	UK layout keyboard
Chinese Traditional	Hong Kong S. A. R., Republic of China (Taiwan)	Chinese Traditional
Chinese Simplified	Mainland of the People's Republic of China	Chinese Simplified
Korean	South Korea	Dubeolsik Hangul
Japanese	Japan	JIS Keyboard
French	France	French (AZERTY) layout keyboard.
German	Germany and Austria	German keyboard (QWERTZ layout)
Belgian	Belgium	Belgian
Norwegian	Norway	Norwegian
Danish	Denmark	Danish
Swedish	Sweden	Swedish
Hungarian	Hungary	Hungarian
Slovenian	Slovenia	Slovenian

Language	Regions	Keyboard layout
Italian	Italy	Italian
Spanish	Spain and most Spanish speaking countries	Spanish

Supported Operating Systems (Clients)

The following operating systems are supported on the 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
Red Hat® Linux 9.0	Yes. Locally held ISO image, Remote File Server mounting directly from KX II-101
Red Hat Enterprise Workstation 3.0 and 4.0	Yes. Locally held ISO image, Remote File Server mounting directly from KX II-101
SUSE Linux Professional 9.2 and 10	Yes. Locally held ISO image, Remote File Server mounting directly from KX II-101
Fedora™ Core 5 and above	Yes. Locally held ISO image, Remote File Server mounting directly from KX II-101
Mac®	No
Solaris	No

Supported Browsers

KX II-101 supports the following browsers:

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

Certified Modems

- US Robotics 56K 5686E
- ZOOM v90
- ZOOM v92
- US Robotics Sportster 56K
- US Robotics Courier 56K

Connectors

Interface type	Length		Description
	Inches	Centimeters	
Video	15"	38 cm	Integrated cable
PS/2	15"	38 cm	Integrated cable
MiniUSB to USB(M)	17.7"	45 cm	Cable for USB
MiniDin9(M) to DB9(F)	72"	182 cm	Cable for serial
DKX2-101-LPKVMC	3.9"	10 cm	Cable for local port integration
DKX2-101-SPDUC	70.86"	180 cm	Cable for connecting to a Dominion PX

TCP and UDP Ports Used

Port	Description
HTTP, Port 80	All requests received by the KX II-101 via HTTP (port 80) are automatically forwarded to HTTPS for complete security. The KX II-101 responds to Port 80 for user convenience, relieving users from having to explicitly type in the URL field to access the KX II-101, while still preserving complete security.
HTTPS, Port 443	This port is used for multiple purposes, including the web server for the HTML client, the download of client software (MPC/KVC) onto the client's host, and the transfer of KVM and virtual media data streams to the client.
KX II-101 (Raritan KVM-over-IP) Protocol, Configurable Port 5000	This port is used to discover other Dominion devices and for communication between Raritan devices and systems, including CC-SG. By default, this is set to Port 5000, but you may configure it to use any TCP port not currently in use. For details on how to configure this setting, see Network Settings (on page 138).
SNTP (Time Server) on Configurable UDP Port 123	The KX II-101 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. Optional
LDAP/LDAPS on Configurable Ports 389 or 636	If the KX II-101 is configured to remotely authenticate user logins via the LDAP/LDAPS protocol, ports 389 or 636 will be used, but the system can also be configured to use any port of your designation. Optional
RADIUS on Configurable Port 1812	If the KX II-101 is configured to remotely authenticate user logins via the RADIUS protocol, either port 1812 will be used, but the system can also be configured to use any port of your designation. Optional
RADIUS Accounting on Configurable Port 1813	If the KX II-101 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 the KX II-101 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	Port 161 is used for inbound/outbound read/write SNMP access and port 162 is used for outbound traffic for SNMP traps. Optional
TCP Port 21	Port 21 is used for the KX II-101 command line interface (when you are working with Raritan Technical Support).

Network Speed Settings

KX II-101 network speed setting

Network switch port setting		Auto	100/Full	100/Half	10/Full	10/Half
Network switch port setting	Auto	Highest Available Speed	KX II-101: 100/Full Switch: 100/Half	100/Half	KX II-101: 10/Full Switch: 10/Half	10/Half
	100/Full	KX II-101: 100/Half Switch: 100/Full	100/Full	KX II-101: 100/Half Switch: 100/Full	No Communication	No Communication
	100/Half	100/Half	KX II-101: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
	10/Full	KX II-101: 10/Half Switch: 10/Full	No Communication	No Communication	10/Full	KX II-101: 10/Half Switch: 10/Full
	10/Half	10/Half	No Communication	No Communication	KX II-101: 10/Full Switch: 10/Half	10/Half

Legend:



Does not function as expected



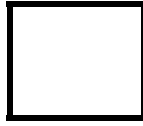
Supported



Functions; not recommended



NOT supported by Ethernet specification; product will communicate, but collisions will occur



Per Ethernet specification, these should be “no communication,” however, note that the KX II-101 behavior deviates from expected behavior

Note: For reliable network communication, configure the KX II-101 and the LAN switch to the same LAN Interface Speed and Duplex. For example, configure both the KX II-101 and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100MB/s/Full.

Admin Port Pinout Information

KX II-101 Admin port			Cable		
MiniDIN9 (Female)	Pin name	I/O	MiniDIN9 (Male)	To PC	DB9F (Female)
1	DCD#	In	1,6	↔	4
2	RXD	In	2	↔	3
3	TXD	Out	3	↔	2
4	DTR#	Out	4	↔	1, 6
5	GND	GND	5	↔	5
6	DSR#	In	1,6	↔	4
7	RTS#	Out	7	↔	8
8	CTS#	In	8	↔	7
9	RI	In	9	↔	9

9 Pin Pinout

15 Pin local port	Pin	Single
	1	LP_RED
	2	LP_GRN
	3	LP_BLU
	4	CN_LP_KB_SDA
	5	CN_LP_KB_SCL
	6	GND
	7	AGND
	8	AGND
	9	+5 V
	10	CN_LP_MS_SDA
	11	CN_LP_MS_SCL
	12	N/C
	13	LP_HS
	14	LP_VS
	15	N/C

Appendix B Updating the LDAP Schema

Note: The procedures in this chapter should be attempted only by experienced users.

In This Chapter

Returning User Group Information	231
Setting the Registry to Permit Write Operations to the Schema	232
Creating a New Attribute	232
Adding Attributes to the Class	233
Updating the Schema Cache.....	235
Editing rciusergroup Attributes for User Members	235

Returning User Group Information

Use the information in this section to return User Group information (and assist with authorization) once authentication is successful.

From LDAP

When an LDAP/LDAPS authentication is successful, the KX II-101 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.

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. See your Microsoft documentation for details.

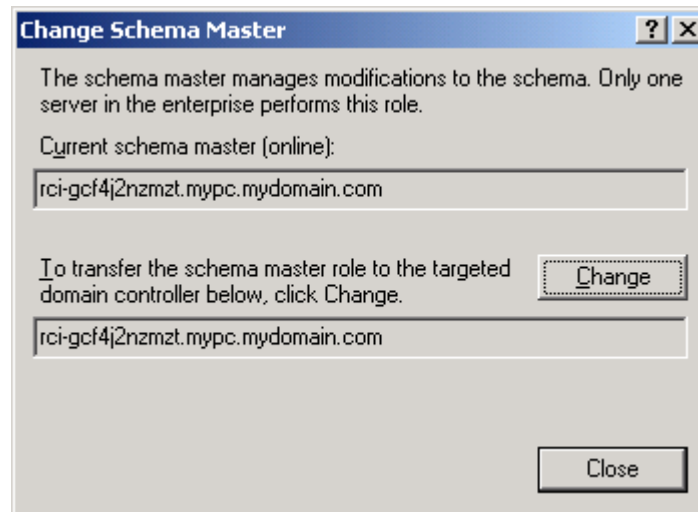
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

► **To permit write operations to the schema:**

1. Right-click the Active Directory Schema root node in the left pane of the window and then click Operations Master. The Change Schema Master dialog appears.



2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**
3. Click OK.

Creating a New Attribute

► **To create new attributes for the rcigroup class:**

1. Click the + symbol before Active Directory Schema in the left pane of the window.
2. Right-click Attributes in the left pane.

- Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.

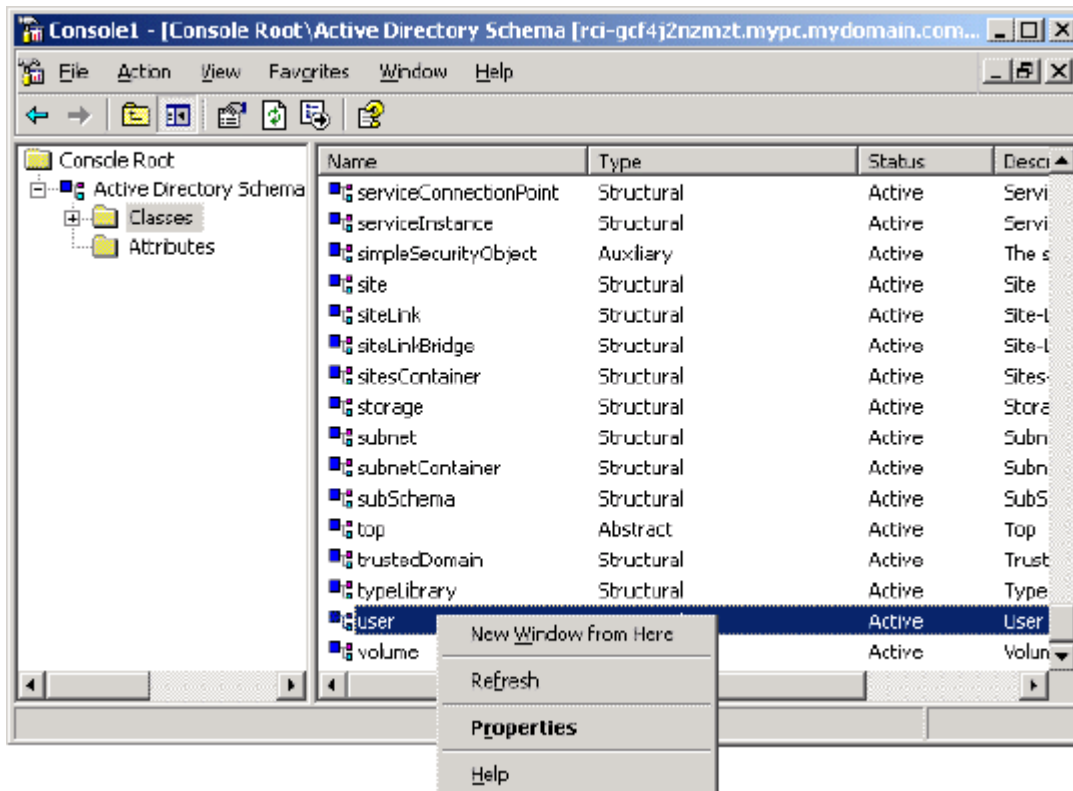
- Type *rciusergroup* in the Common Name field.
- Type *rciusergroup* in the LDAP Display Name field.
- Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
- Type a meaningful description in the Description field.
- Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
- Type *1* in the Minimum field.
- Type *24* in the Maximum field.
- Click OK to create the new attribute.

Adding Attributes to the Class

► **To add attributes to the class:**

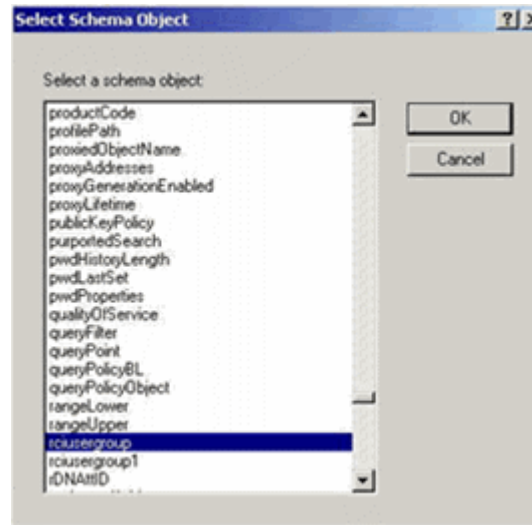
- Click Classes in the left pane of the window.

2. Scroll to the user class in the right pane and right-click it.



3. Choose Properties from the menu. The user Properties dialog appears.
4. Click the Attributes tab to open it.
5. Click Add.

- Choose rcigroup from the Select Schema Object list.



- Click OK in the Select Schema Object dialog.
- Click OK in the User Properties dialog.

Updating the Schema Cache

► **To update the schema cache:**

- Right-click Active Directory Schema in the left pane of the window and select Reload the Schema.
- Minimize the Active Directory Schema MMC (Microsoft Management Console) console.

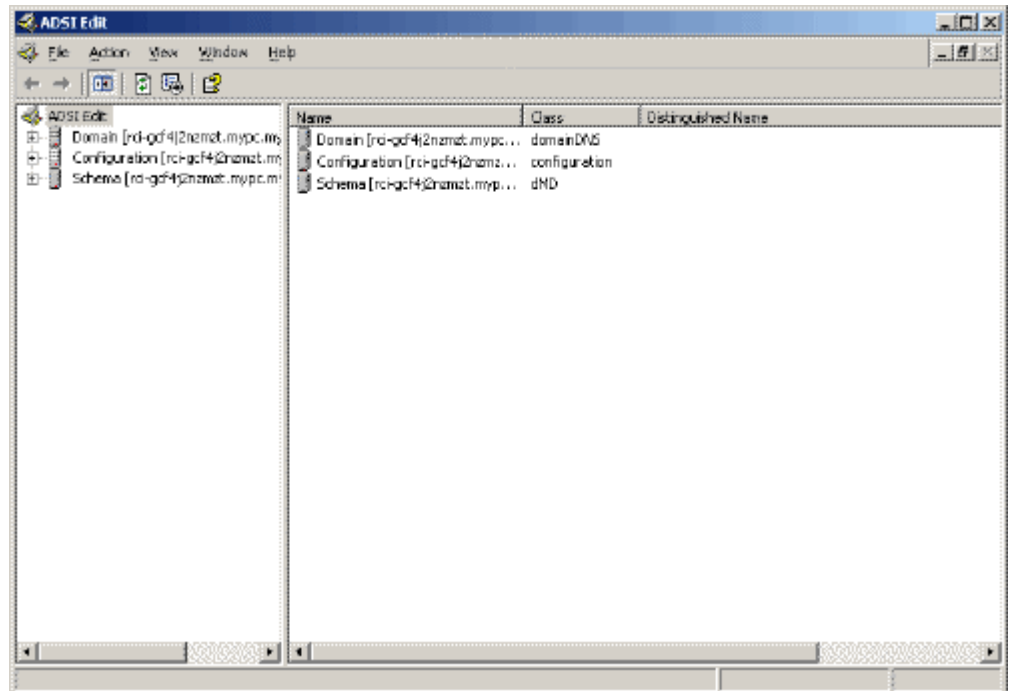
Editing rcigroup Attributes for User Members

To run the Active Directory script on Windows 2003 server, use the script provided by Microsoft (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

► **To edit the individual user attributes within the group rcigroup:**

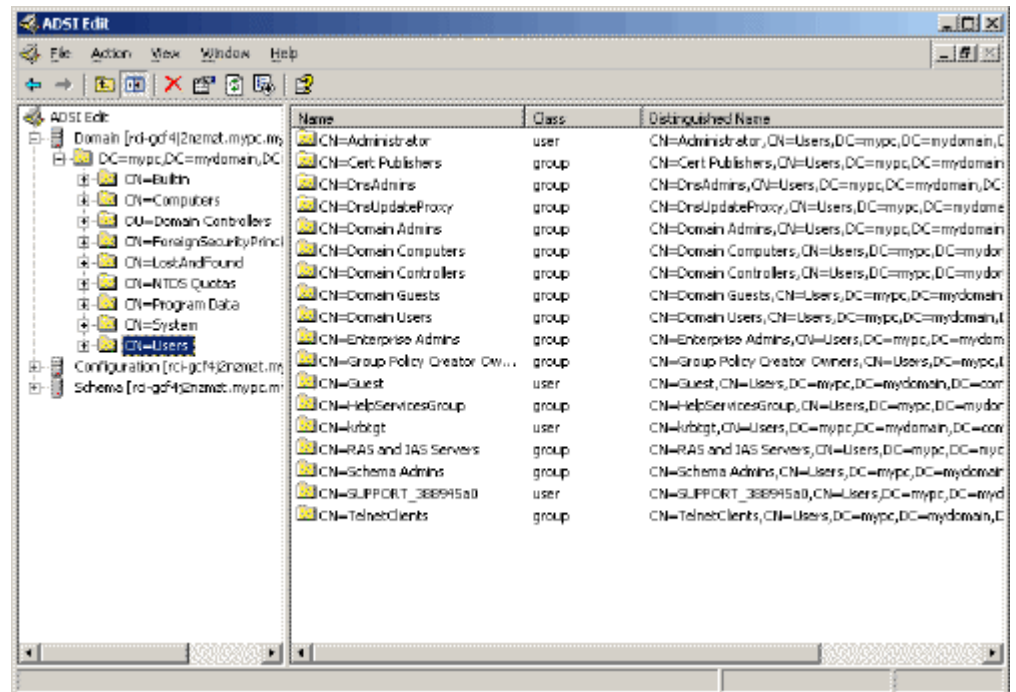
- From the installation CD, choose Support > Tools.
- Double-click SUPTOOLS.MSI to install the support tools.

3. Go to the directory where the support tools were installed. Run `adsiedit.msc`. The ADSI Edit window opens.



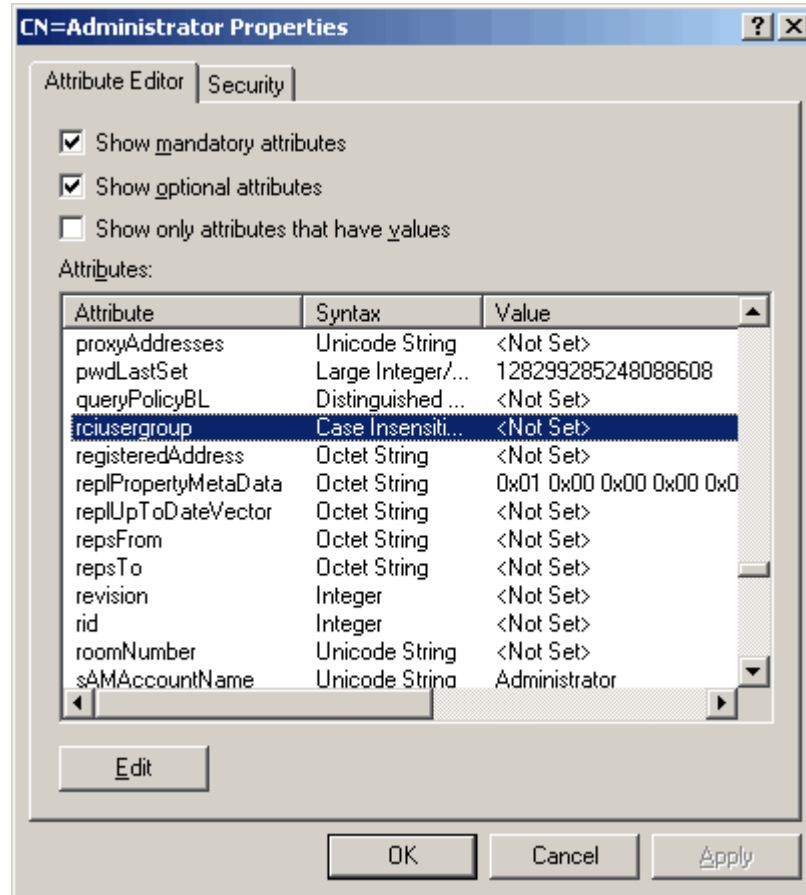
4. Open the Domain.

- In the left pane of the window, select the CN=Users folder.

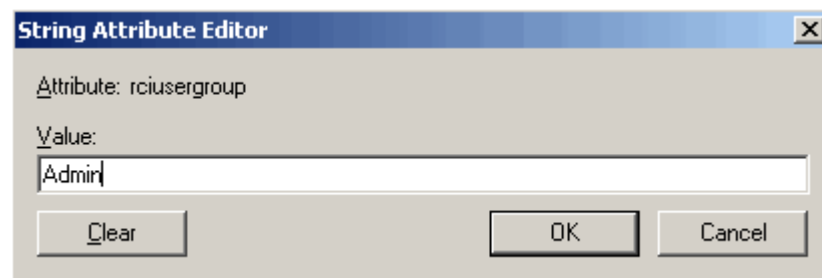


- Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.

- Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.



- Click Edit. The String Attribute Editor dialog appears.
- Type the user group (created in the KX II-101) in the Edit Attribute field.



- Click OK.

Appendix C AC-DC Adapter and Rack Mount

The KX II-101 device can be mounted vertically or horizontally, facing the front or the rear, on either side of a server rack. Use the brackets and screws included with the KX II-101 kit.

In This Chapter

AC-DC Adapter Clip Fitting.....239
Bracket Installation241

AC-DC Adapter Clip Fitting

Identify the Clip Type






Diagram key	
	EU clip
	Australian clip

Diagram key	
	UK clip

Remove the Attachment Cover from AC-DC Power Adapter

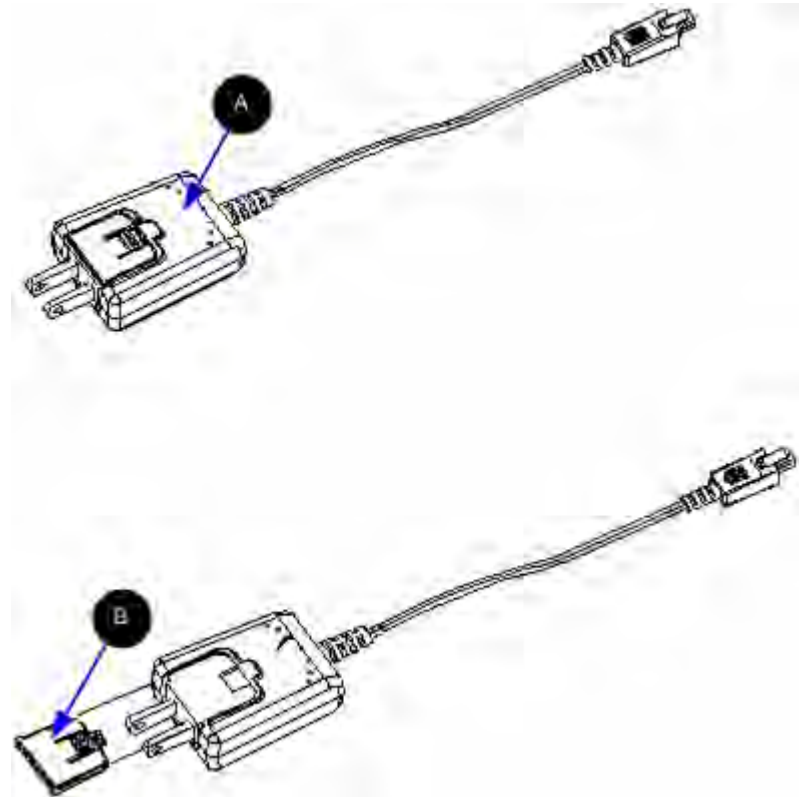




Diagram key	
	AC/DC power adaptor
	Attachment cover. Push to remove.

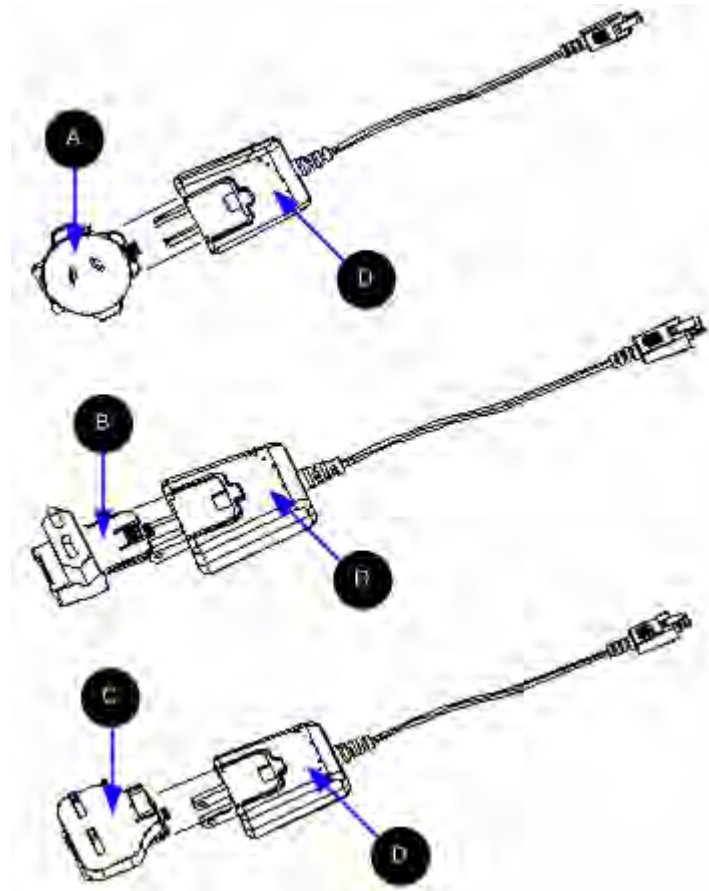
Attach the Clip to AC-DC Power Adapter

Diagram key	
A	Australian clip
B	EU clip
C	UK clip
D	Power adaptor

Bracket Installation

1. Remove the screws from the KX II-101.

- Slide the left and right panels off the KX II-101.

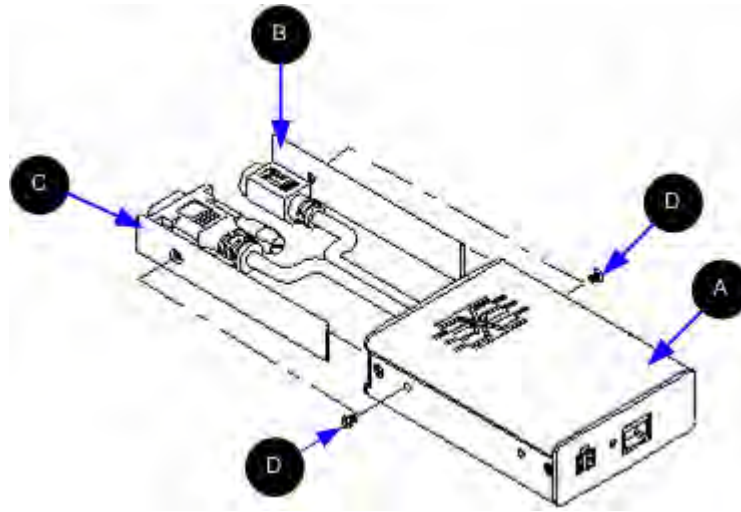


Diagram key

A	KX II-101
B	Right panel
C	Left panel
D	Screws

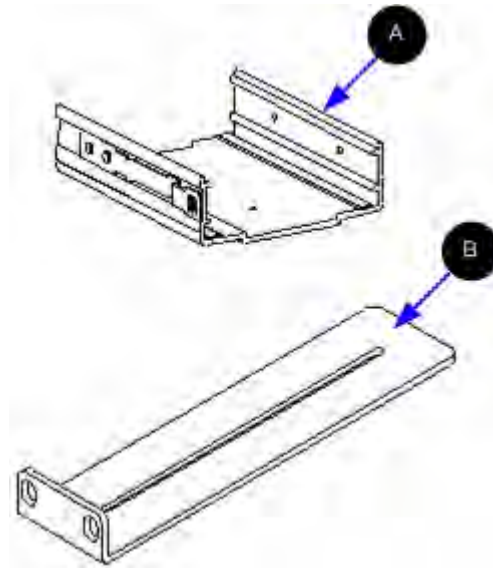
KX II-101 Bracket Parts


Diagram key	
A	U bracket
B	L bracket

Attach the Brackets to KX II-101 for Horizontal Mount

1. Attach the U bracket to the L bracket using the included screws. Adjust bracket placement before tightening screws.
2. Mount the U and L bracket assembly to the rack with rack-mount screws (provided by the rack manufacturer).
3. Slide the KX II-101 into the U bracket with the KVM harness facing towards the target. Pull and release the latch lever to lock the KX II-101 into the U bracket.

This image illustrates mounting the KX II-101 on the left. To mount the KX II-101 on the right, follow these directions but attach brackets to the right side of the KX II-101.

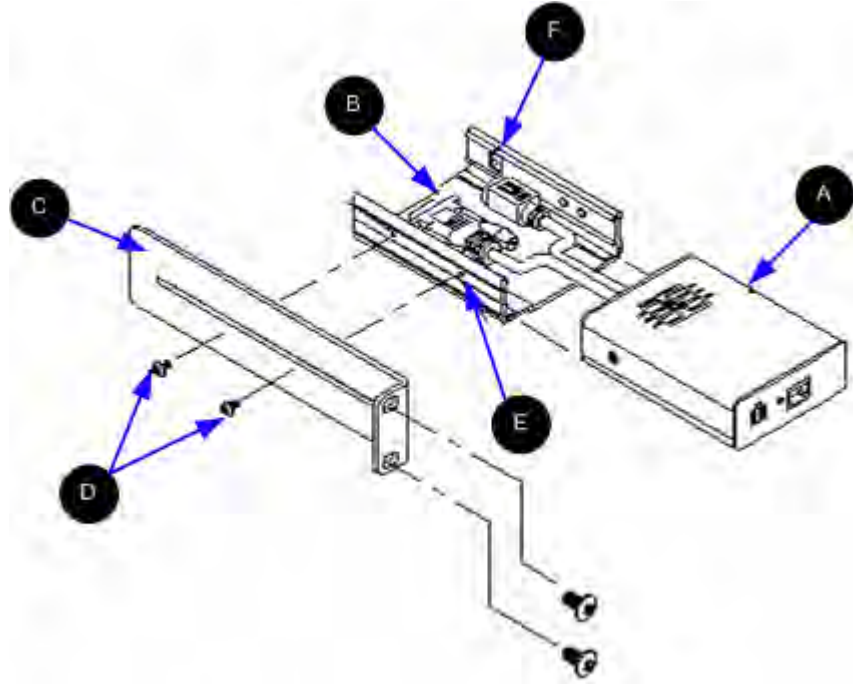


Diagram key	
A	KX II-101
B	U bracket
C	L bracket
D	Screws
E	Mounting hole
F	Latch lever

Attach the Brackets to KX II-101 for Vertical Mount

1. Attach the U bracket to the L bracket using the included screws. Adjust bracket placement before tightening screws.

2. Mount the U and L bracket assembly to the rack with rack-mount screws (provided by the rack manufacturer).
3. Slide the KX II-101 device into the U bracket with the KVM harness facing towards the target. Pull and release the latch lever to lock the KX II-101 device into the U bracket.

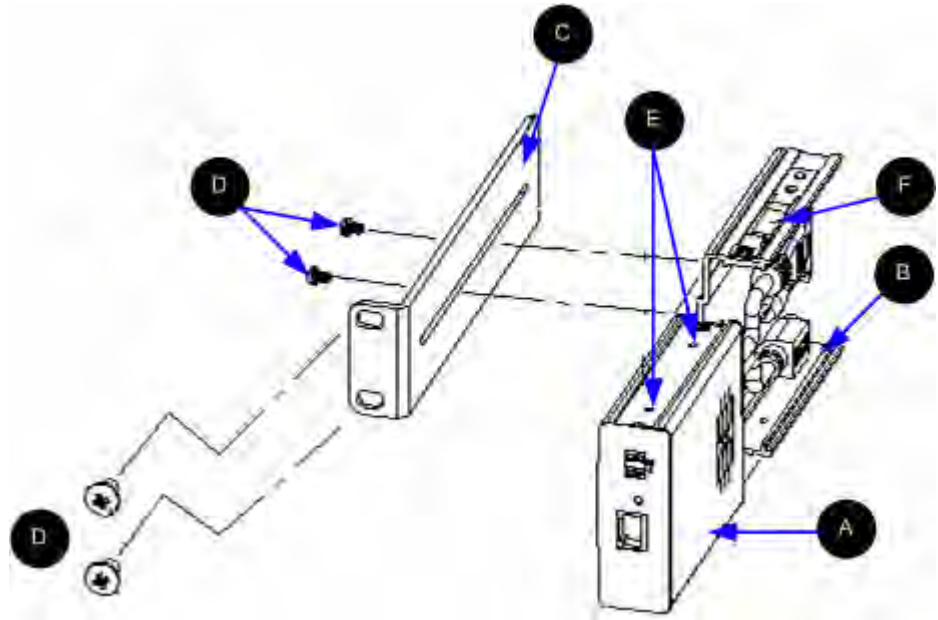


Diagram key	
A	KX II-101
B	U bracket
C	L bracket
D	Screws
E	Mounting hole
F	Latch lever

Appendix D Informational Notes

In This Chapter

Java Runtime Environment (JRE)	246
Keyboard, Video and Mouse Notes.....	246

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 KVM and Serial Access Clients User Guide for more information.

The KX II-101 Remote Console and MPC require the JRE to function. The KX II-101 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 JRE version 1.5 for optimum performance, but the KX II-101 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.x except for 1.6.2.

Note: For multi-language keyboards to work in the KX II-101 Remote Console (Virtual KVM Client), please install the multi-language version of Java Runtime Environment (JRE).

Keyboard, Video and Mouse Notes

The following equipment have certain keyboard, video, or mouse limitations. Where applicable, a workaround is supplied.

Sun Blade™ Video, Keyboard, and Mouse Support Limitation

Video

If you are accessing a Sun Blade 100 with the KX II-101, video on the local port or a remote connection when the Sun Blade is booting up.

To avoid this issue, be sure you are using Sun Open Boot firmware 4.17.1 or later.

Keyboard and Mouse

Since Sun Blades do not support multiple keyboards, and no local keyboard or mouse port is provided, a KX II-101 and local keyboard cannot be used at the same time. However, a remote keyboard and mouse can be used for Sun Blades.

Sun Keyboard Key Support Limitations

The following keys on Sun keyboards are not supported by KX II-101:

Sun key	Local port key combination
Again	Ctrl+ Alt +F2
Props	Ctrl + Alt +F3
Undo	Ctrl + Alt +F4
Stop A	Break a
Front	Ctrl + Alt + F5
Copy	Ctrl + Alt + F6
Open	Ctrl + Alt + F7
Find	Ctrl + Alt + F9
Cut	Ctrl + Alt + F10
Paste	Ctrl + Alt + F8
Mute	Ctrl + Alt + F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	No key combination
Power	No key combination

BIOS Access Limitation from a Local Keyboard

A USB connection is required when using Absolute Mouse Synchronization. However, the keyboards in this section do not support a USB connection to the local keyboard. To access the local keyboard via BIOS or virtual media through the local port, follow these configurations:

Keyboard	Configuration to use
Dell Optiplex GX280 - BIOS A03	<p>BIOS and virtual media can be accessed for local and remote keyboards using a Newlink USB to PS/2 adapter.</p> <p>Set the Host Interface to PS/2 on the Keyboard/Mouse Setup page. See Keyboard/Mouse Setup (on page 143).</p>

Keyboard	Configuration to use
Dell Dimension 2400– BIOS A05	Set the Host Interface to PS/2 on the Keyboard/Mouse Setup page. See Keyboard/Mouse Setup (on page 143).
Dell Optiplex 170L - BIOS A07	PS/2 plus a PS/2-to-USB-adapter. Set the Host Interface to PS/2 on the Keyboard/Mouse Setup page. See Keyboard/Mouse Setup (on page 143).
Dell Server 1850	In order for BIOS version A06 to recognize a virtual media mounted removable USB flash drive, use the PS/2 and USB connections between the Dell server and the KX II-101. Set the Host Interface to PS/2 on the Keyboard/Mouse Setup page. See Keyboard/Mouse Setup (on page 143).

HP UX RX 1600 Keyboard and Mouse Configuration

If you are using an HP UX RX 1600 running UNIX, do the following to connect the device to the target:

- Verify you are using KX II-101 firmware 2.0.20.5.6964 or higher.
- Use the USB cable that is supplied with the KX II-101 .
- Set the Host Interface field on the Keyboard/Mouse Setup page to USB. See **Keyboard/Mouse Setup** (on page 143).
- Verify that the Enable Absolute Mouse and Use Full Speed checkboxes on the Port page are not selected. See **Port Configuration** (on page 154).
- Use either Intelligent or Standard Mouse mode. Do not use Absolute Mouse mode.

Compaq Alpha and IBM P Server Mouse Mode Limitation

When connecting to either Compaq Alpha servers or IBM P servers through the KX II-101, you must use Single Mouse mode. See **Working with Target Servers** (on page 32).

Windows 2000 and 2003 Server Keyboard Limitations

Due to an operating system limitation, the following keyboard combinations do not work with a US-International keyboard layout when using Windows 2000 and Windows 2003 servers.

- Right Alt+D
- Right Alt+I
- Right Alt+L

Note: Right Alt may be labeled as AltGr on keyboards that specifically have US/International markings on the keys.

Index

9

9 Pin Pinout • 230

A

Absolute Mouse Mode • 54, 92
Accessing the KX II-101 Using the CLI • 211
AC-DC Adapter and Rack Mount • 6, 239
AC-DC Adapter Clip Fitting • 239
Adding a New User • 124, 125
Adding a New User Group • 118, 124
Adding Attributes to the Class • 233
Adding, Deleting, and Editing Favorites • 39
Admin Port • 23, 29, 144
Admin Port Pinout Information • 229
Administration Features • 5
Administrative Functions • 99
Advanced USB Connection Settings • 168
Analog KVM Switch • 1, 144, 162
Apple Macintosh® Settings • 15
Assigning an IP Address • 10, 25
Attach the Brackets to KX II-101 for Horizontal Mount • 243
Attach the Brackets to KX II-101 for Vertical Mount • 244
Attach the Clip to AC-DC Power Adapter • 241
Audit Log • 195
Authentication Settings • 126
Auto-Scroll • 74
Auto-Sense Video Settings • 49

B

Backing Up and Restoring a Device Configuration • 103
Backing Up and Restoring a User Configuration • 104
Backup and Restore • 197
Backup and Restore Functions • 103
Basic USB Connection Settings • 166
BIOS Access Limitation from a Local Keyboard • 247
Blocking and Unblocking Users • 125
Bracket Installation • 241
Broadcast Port • 104
Building a Keyboard Macro • 46, 82

C

Calibrate Color • 50

CC Unmanage • 219
CD-ROM/DVD-ROM/ISO Images • 111, 114
Certified Modems • 147, 226
Changing a Password • 102, 137
Changing the Shortcut Menu Keyboard Combination • 79, 80
Checking Your Browser for AES Encryption • 191, 192
CLI Commands • 210, 214
CLI Prompts • 213
CLI Syntax -Tips and Shortcuts • 214
Closing a Remote Connection • 78
Color Calibration • 98
Command Line Interface (CLI) • 144, 210
Common Commands for All Command Line Interface Levels • 214
Common Hot Key Exceptions for MPC • 86
Compaq Alpha and IBM P Server Mouse Mode Limitation • 248
Completion of Commands • 213
Conditions when Read/Write is Not Available • 113, 114
Configuration • 216
Configure the KX II-101 Using a Terminal Emulation Program (Optional) • 10, 23, 24, 29, 212
Configure the KX II-101 Using the Remote Console • 24
Configuring Direct Port Access • 26
Configuring Event Management - Settings • 150, 151
Connecting the Power Strip • 155, 157
Connecting to a KVM Target Server • 41
Connecting to a Remote KVM Console • 78
Connecting to Virtual Media • 113
Connection and Video Properties • 94
Connection Information • 45, 77
Connection Profiles • 62, 74
Connectors • 7, 226
Controlling a Power Strip Device • 157, 160, 161
Create User Groups and Users • 29
Creating a New Attribute • 232
Creating, Modifying and Deleting Profiles in MPC • 74, 147
Ctrl+Alt+Del Macro • 86
Customizing the Navigator • 63

D

Date/Time Settings • 148
 Debug • 215, 216
 Default Logon Information • 9
 Device Diagnostics • 208
 Device Information • 196
 Device Management • 27, 138
 Device Ports in the Navigator • 62
 Device Services • 141, 211
 Devices in the MPC Navigator • 62
 Diagnostics • 202, 215
 Disconnecting a KVM Target Server • 43
 Disconnecting Virtual Media • 115
 Discovering Raritan Devices on the KX II-101 Subnet • 39
 Discovering Raritan Devices on the Local Subnet • 37

E

Editing rcusergroup Attributes for User Members • 235
 Enable Direct Port Access • 32
 Encryption & Share • 163, 184, 190
 Establishing a New Connection • 76
 Event Management • 149
 Event Management - Destinations • 151

F

Favorites List Page • 37, 39
 File Server Setup (File Server ISO Images Only) • 111, 115
 From LDAP • 231
 From Microsoft Active Directory • 231

G

General Options in MPC • 99, 100
 Generation 2 Devices • 77
 Getting Started • 10
 Group-Based IP ACL (Access Control List) • 118, 120, 123

H

Help Options • 59
 HP UX RX 1600 Keyboard and Mouse Configuration • 248

I

IBM AIX® Settings • 15
 Identify the Clip Type • 239

Implementing LDAP/LDAPS Remote Authentication • 127, 130
 Implementing RADIUS Remote Authentication • 126, 130
 Informational Notes • 246
 Installation and Configuration • 9, 217
 Intelligent Mouse Mode • 55, 92, 93
 Interface Command • 217
 Interfaces • 5, 32
 Introduction • 1
 IP Access Control • 193

J

Java Runtime Environment (JRE) • 246

K

Keyboard Limitations • 89
 Keyboard Macros • 46, 82
 Keyboard Options • 46
 Keyboard Type • 88
 Keyboard, Video and Mouse Notes • 246
 Keyboard/Mouse Setup • 143, 162, 247, 248
 Known USB Profiles • 166, 168, 169
 KX II-101 Bracket Parts • 243
 KX II-101 Console Navigation • 33
 KX II-101 Overview • 2
 KX II-101 Remote Console Interface • 32, 33
 KX II-101 Specifications • 222

L

LAN Interface Settings • 138, 140
 Linux® Settings • 14
 Listports Command • 215, 218
 Local Drives • 113
 Local User Port • 24
 Logging off • 41
 Logging On • 211, 212
 Logon Limitations • 184, 185

M

Maintenance • 195
 Manage Favorites Page • 37
 Managing Favorites • 36
 Managing KVM Target Servers (Port Page) • 155, 157
 Managing Power Associations • 159
 Managing USB Connections • 1, 165
 Modem • 146
 Modem Access Cable Connections • 147, 148
 Modifying an Existing User • 125

- Modifying an Existing User Group • 123
- Modifying and Removing Keyboard Macros • 48, 86
- Mounting • 6
- Mouse Modes • 12
- Mouse Options • 52, 91, 100
- Mouse Pointer Synchronization • 53
- Mouse Synchronization Options • 92
- MPC Broadcast Port • 104
- MPC Connected Server(s) Toolbar • 68
- MPC Connection Properties • 94
- MPC Interface • 60
- MPC Navigator Tabs • 64
- MPC Scaling • 73
- MPC Status Bar • 69
- MPC Target Screen Resolution Mode • 71
- Multi-Platform Client (MPC) • 41, 60
- Multi-Platform Client Interface • 41

N

- Name Command • 215, 217
- Naming the Power Strip (Port Page for Power Strips) • 157, 158
- Naming the Target Server • 27
- Navigation of the CLI • 212
- Navigator • 61
- Navigator Display Options • 65
- Navigator Icons • 62
- Network • 23, 215, 217
- Network Basic Settings • 138, 139
- Network Configuration • 5
- Network Interface Page • 202
- Network Settings • 138, 227
- Network Speed Settings • 141, 228
- Network Statistics Page • 203
- Note on Microsoft Active Directory • 29
- Note to CC-SG Users • 28
- Note to MPC Users • 99

O

- Operation • 60
- Optional Accessories • 7
- Overview • 9, 41, 107, 166, 210, 219

P

- Package Contents • 7
- Ping Host Page • 206
- Port Access Page • 34
- Port Action Menu • 34
- Port Configuration • 15, 154, 248

- Power • 6, 18
- Power Control • 42, 155, 157
- Power Controlling a KVM Target Server • 42
- Prerequisites for Using Virtual Media • 110
- Product Features • 5
- Product Photos • 4
- PS/2 Configuration • 21

R

- RADIUS Communication Exchange Specifications • 133
- Raritan Power Strip Control • 145
- Rebooting • 201
- Refresh Screen • 49
- Related Documentation • 8
- Relationship Between Users and Groups • 117
- Remote Authentication • 28
- Remote Power Management • 105
- Remove the Attachment Cover from AC-DC Power Adapter • 240
- Removing a KX II-101 from CC-SG Management • 220
- Renaming a Port • 156
- Requirements and Installation • 60
- Resetting the KX II-101 Using the Reset Button • 163, 192
- Restarting a Device • 103
- Returning User Group Information • 231
- Returning User Group Information from Active Directory Server • 129
- Returning User Group Information via RADIUS • 133
- Running a Keyboard Macro • 48, 85

S

- Screen Modes • 70
- Security Management • 184
- Security Settings • 124, 184
- Serial Port Settings • 144
- Setlog Command • 215, 216
- Setting a New Password • 24
- Setting Permissions • 118, 122, 123
- Setting Permissions for an Individual Group • 122, 125
- Setting Port Permissions • 118, 119, 123
- Setting the Registry to Permit Write Operations to the Schema • 232
- Setting the Server Video Resolution • 10, 11
- Shortcut Menu • 79, 86, 101
- Shortcut Menu Key Options • 80

Index

- Single Cursor Mode/Dual Cursor Mode • 91
- Single Mouse Cursor • 56
- Specifications • 1, 222
- Specifying a Keyboard Type in MPC • 88
- SSH Access from a UNIX/Linux Workstation • 212
- SSH Access from a Windows PC • 211
- SSH Connection to the KX II-101 • 211
- Standard Mouse Mode • 54, 92, 94
- Standard Toolbar • 65
- Step 1
 - Configure the Target Server • 9, 10
- Step 2
 - Configure Network Firewall Settings • 9, 16
- Step 3
 - Connect the KX II-101 • 9, 17
- Step 4
 - Configure the KX II-101 • 9, 24
- Strong Passwords • 137, 184, 186
- Sun Blade™ Video, Keyboard, and Mouse Support Limitation • 246
- Sun Keyboard Key Support Limitations • 247
- Sun® Solaris™ Settings • 14
- Sun™ Video Resolution • 11
- Supported Browsers • 225
- Supported Keyboard Languages • 224
- Supported Operating Systems (Clients) • 225
- Supported Protocols • 28
- Supported Video Resolutions • 223
- System Management Features • 5

T

- Target Server • 19
- TCP and UDP Ports Used • 226
- Terminology • 6
- Tool Options • 57
- Toolbars • 65
- Trace Route to Host Page • 206

U

- Updating the LDAP Schema • 129, 231
- Updating the Schema Cache • 235
- Upgrade History • 200
- Upgrading Device Firmware • 102
- Upgrading Firmware • 198
- USB Configuration • 19
- User Authentication Process • 135
- User Blocking • 125, 184, 188
- User Features • 6
- User Group List • 117

- User Groups • 116
- User Guide • 7
- User List • 124
- User Management • 29, 116
- Userlist Command • 215, 218
- Users • 123
- Using CC-SG in Proxy Mode • 221

V

- Video Properties • 49
- Video Resolution • 6
- Video Settings - Generation 2 Devices • 95
- View Options • 59
- Virtual KVM Client • 34, 41
- Virtual Media • 56, 106
- VKC Connection Properties • 43
- VKC Toolbar • 42
- VKC Video Settings • 50
- VKC Virtual Media • 56

W

- What's New in the User Guide • 1
- Windows 2000 and 2003 Server Keyboard Limitations • 249
- Windows 2000® Settings • 12
- Windows Key in MPC • 87
- Windows Vista® Settings • 13
- Windows XP®/Windows 2003® Settings • 13
- Working with Target Servers • 32, 248

▶ **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

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

▶ **India**

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

▶ **Japan**

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5994
Email: support.japan@raritan.com

▶ **Europe**

Europe

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom

Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0

▶ **Korea**

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +82-2-5578730

▶ **Melbourne, Australia**

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

▶ **Taiwan**

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: tech.rap@raritan.com