



Dominion KX II-101

User Guide

2.0.40

Copyright © 2009 Raritan, Inc.

KX2101-v2.40-0C-E

September 2009

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 2009 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 Help.....	1
KX II-101 Help.....	1
Related Documentation.....	2
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
Chapter 2 Installation and Configuration	8
Overview.....	8
Default Login Information.....	8
Getting Started.....	9
Step 1: Configure the Target Server.....	9
Step 2: Configure Network Firewall Settings.....	15
Step 3: Connect the KX II-101.....	16
Step 4: Configure the KX II-101.....	23
Chapter 3 Working with Target Servers	31
Interfaces.....	31
KX II-101 Remote Console Interface.....	31
Multi-Platform Client Interface.....	40
Virtual KVM Client.....	40
Overview.....	40
Connecting to a KVM Target Server.....	40
VKC Toolbar for the KX II-101.....	41
Power Controlling a KVM Target Server.....	41
Disconnecting a KVM Target Server.....	42
VKC Connection Properties.....	43
Connection Information.....	45

Keyboard Options.....	45
Video Properties	48
Mouse Options.....	52
VKC Virtual Media	56
Tool Options	57
View Options.....	59
Help Options	60

Chapter 4 Virtual Media 61

Overview	62
Prerequisites for Using Virtual Media	65
File Server Setup (File Server ISO Images Only).....	66
Using Virtual Media.....	67
Connecting to Virtual Media.....	68
Local Drives	68
Conditions when Read/Write is Not Available	69
CD-ROM/DVD-ROM/ISO Images.....	69
Disconnecting Virtual Media	71

Chapter 5 User Management 72

User Groups.....	72
User Group List.....	73
Relationship Between Users and Groups	73
Adding a New User Group.....	73
Modifying an Existing User Group	78
Users.....	79
User List.....	79
Adding a New User	80
Modifying an Existing User	80
Blocking and Unblocking Users.....	81
Authentication Settings	81
Implementing LDAP/LDAPS Remote Authentication	82
Returning User Group Information from Active Directory Server	84
Implementing RADIUS Remote Authentication.....	85
Returning User Group Information via RADIUS.....	90
RADIUS Communication Exchange Specifications.....	90
User Authentication Process	92
Changing a Password.....	97

Chapter 6 Device Management 98

Network Settings.....	98
Network Basic Settings.....	99
LAN Interface Settings.....	100
Device Services	101
Keyboard/Mouse Setup	103
Serial Port Settings	104
Admin Port.....	104

Raritan Power Strip Control	105
Modem	106
Date/Time Settings	108
Event Management	109
Configuring Event Management - Settings	110
Event Management - Destinations	111
Port Configuration	115
Managing KVM Target Servers (Port Page)	116
Power Control	118
Analog KVM Switch	123
Resetting the KX II-101 Using the Reset Button	124

Chapter 7 Managing USB Connections 126

Overview	127
Basic USB Connection Settings	127
Advanced USB Connection Settings	129

Chapter 8 Security Management 131

Security Settings	131
Login Limitations	132
Strong Passwords	133
User Blocking	134
Encryption & Share	135

IP Access Control	139
Chapter 9 Maintenance	142
Audit Log	142
Device Information	143
Backup and Restore	144
Upgrading Firmware	146
Upgrade History	148
Factory Reset.....	148
Rebooting.....	149
Chapter 10 Diagnostics	151
Network Interface Page	151
Network Statistics Page	151
Ping Host Page	153
Trace Route to Host Page	154
Device Diagnostics	155
Chapter 11 Command Line Interface (CLI)	157
Overview	157
Accessing the KX II-101 Using the CLI.....	158
SSH Connection to the KX II-101	158
SSH Access from a Windows PC (Shared KSX II, KX II 101, SX).....	158
SSH Access from a UNIX/Linux Workstation	159
SSH Access when Alternate RADIUS Authentication is Enabled	159
Logging On	159
Navigation of the CLI	160
CLI Prompts.....	160
Completion of Commands	161
CLI Syntax -Tips and Shortcuts.....	161
Common Commands for All Command Line Interface Levels	161
CLI Commands	162
Diagnostics	163
Configuration	164
Listports Command	166
Userlist Command	166

Chapter 12 CC Unmanage	167
Overview	167
Removing a KX II-101 from CC-SG Management.....	168
Using CC-SG in Proxy Mode	169
Appendix A Specifications	170
KX II-101 Specifications.....	170
Supported Video Resolutions	171
Supported Keyboard Languages	172
Supported Operating Systems (Clients)	173
Supported Browsers	175
Certified Modems.....	175
Connectors.....	175
TCP and UDP Ports Used	175
Network Speed Settings	177
Admin Port Pinout Information.....	178
9 Pin Pinout.....	178
Appendix B Updating the LDAP Schema	180
Returning User Group Information.....	180
From LDAP	180
From Microsoft Active Directory	180
Setting the Registry to Permit Write Operations to the Schema	181
Creating a New Attribute.....	181
Adding Attributes to the Class	182
Updating the Schema Cache.....	184
Editing rciusergroup Attributes for User Members.....	184
Appendix C AC-DC Adapter and Rack Mount	187
AC-DC Adapter Clip Fitting	187
Identify the Clip Type	187
Remove the Attachment Cover from AC-DC Power Adapter.....	188
Attach the Clip to AC-DC Power Adapter.....	189
Bracket Installation.....	189
KX II-101 Bracket Parts	191
Attach the Brackets to KX II-101 for Horizontal Mount.....	191
Attach the Brackets to KX II-101 for Vertical Mount	192
Appendix D Informational Notes	194
Java Runtime Environment (JRE)	194
Keyboard, Video and Mouse Notes	194
Sun Blade™ Video, Keyboard, and Mouse Support Limitation.....	194

Contents

Sun Keyboard Key Support Limitations.....	195
BIOS Access Limitation from a Local Keyboard.....	195
HP UX RX 1600 Keyboard and Mouse Configuration.....	196
Compaq Alpha and IBM P Server Mouse Mode Limitation.....	196
Windows 2000 and 2003 Server Keyboard Limitations.....	197

Index

199

Chapter 1 Introduction

In This Chapter

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

What's New in the Help

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

- The KX II-101 now supports alternate RADIUS authentication through the local serial port, KVM client and SSH. See **Admin Port** (on page 22), **Connecting to a KVM Target Server** (on page 40), **Implementing RADIUS Remote Authentication** (on page 85), **User Authentication Process** (on page 92) and **SSH Access when Alternate RADIUS Authentication is Enabled** (on page 159).
- The KX II-101 now supports the use of FIPS compliant algorithms. To support FIPS, see **Encryption & Share** (on page 135) for information on an encryption setting that must be enabled.

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

KX II-101 Help

The KX II-101 help 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.

A PDF version of the help can be downloaded from the **Raritan Firmware and Documentation page** <http://www.raritan.com/support/firmware-and-documentation/> on the Raritan website. Raritan recommends that you refer to the Raritan website for the most up-to-date user guides available.

Note: In order to use online help, Active Content must be enabled in your browser. Consult your browser help for information on enabling active content.

Related Documentation

The KX II-101 help is accompanied by a KX II-101 Quick Setup Guide, which can be found on the **Raritan Firmware and Documentation page** <http://www.raritan.com/support/firmware-and-documentation/> of Raritan's website. Installation requirements and instructions for client applications used with the KX II-101 can be found in the **KVM and Serial Access Clients Guide**, also found on the Raritan website. Where applicable, specific client functions used with the KX II-101 are included in the help.

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.

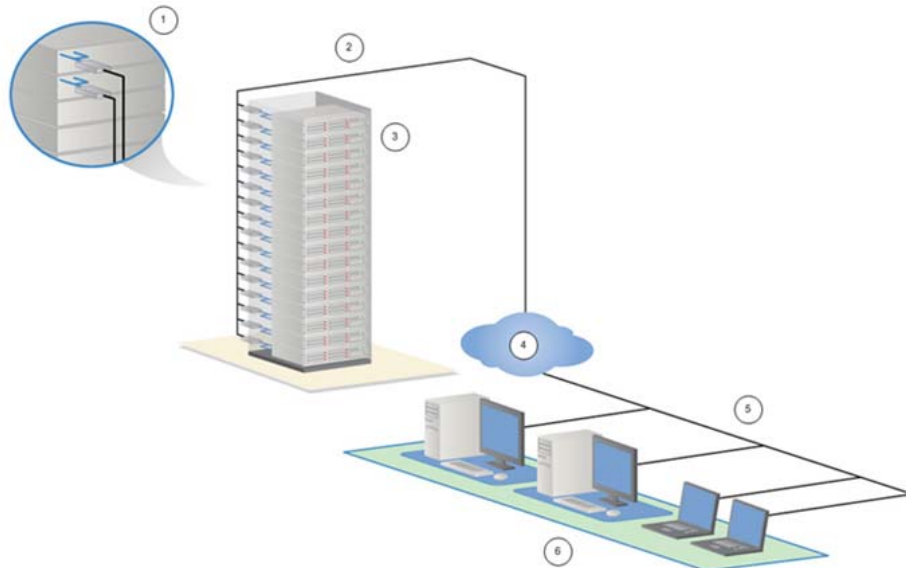





Diagram key	
①	KX II-101
②	LAN
③	Windows, Linux, and Sun servers
④	TCP/IP
⑤	LAN
⑥	Remote (network) access

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 187).

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.
Local User port	Enables a user in immediate proximity to the target server to use the native keyboard and mouse

Term	Description
	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
- 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 175).

Chapter 2 Installation and Configuration

In This Chapter

Overview	8
Default Login Information	8
Getting Started	9

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 9)
- **Step 2: Configure Network Firewall Settings** (on page 15)
- **Step 3: Connect the KX II-101** (on page 16)
- **Step 4: Configure the KX II-101** (on page 23)

In order to ensure optimum performance, before installing the KX II-101 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 Login 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 24) 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 28) 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 9).

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.

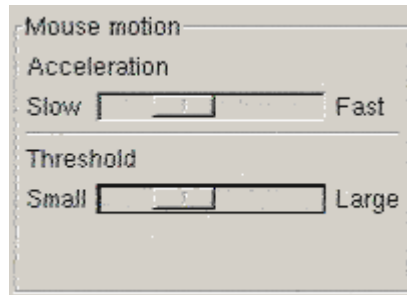
Note: In many Linux graphical environments, the command `Ctrl+Alt+ +` (plus sign) changes the video resolution, scrolling through all available resolutions that remain enabled in the XF86Config file.

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 115).

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		
A	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.
B	Monitor and PS/2 cable	Attached Monitor and PS/2 cable (see E).
C	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.
D	Power indicator	Backlit LED power ON and boot-up indicator. Provides feedback on the operating status of the device.
E	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.
F	Power connector	Connects the power supply if you are not using a PoE (Power over Ethernet) LAN connection.
G	Local user port	Use to connect a local keyboard, video, and mouse directly to the target server using an optional PS/2 cable.
H	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. **Sold Separately**

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

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

Note: To ensure the best connectivity using a USB cable, only use the USB cable provided with the KX II-101.

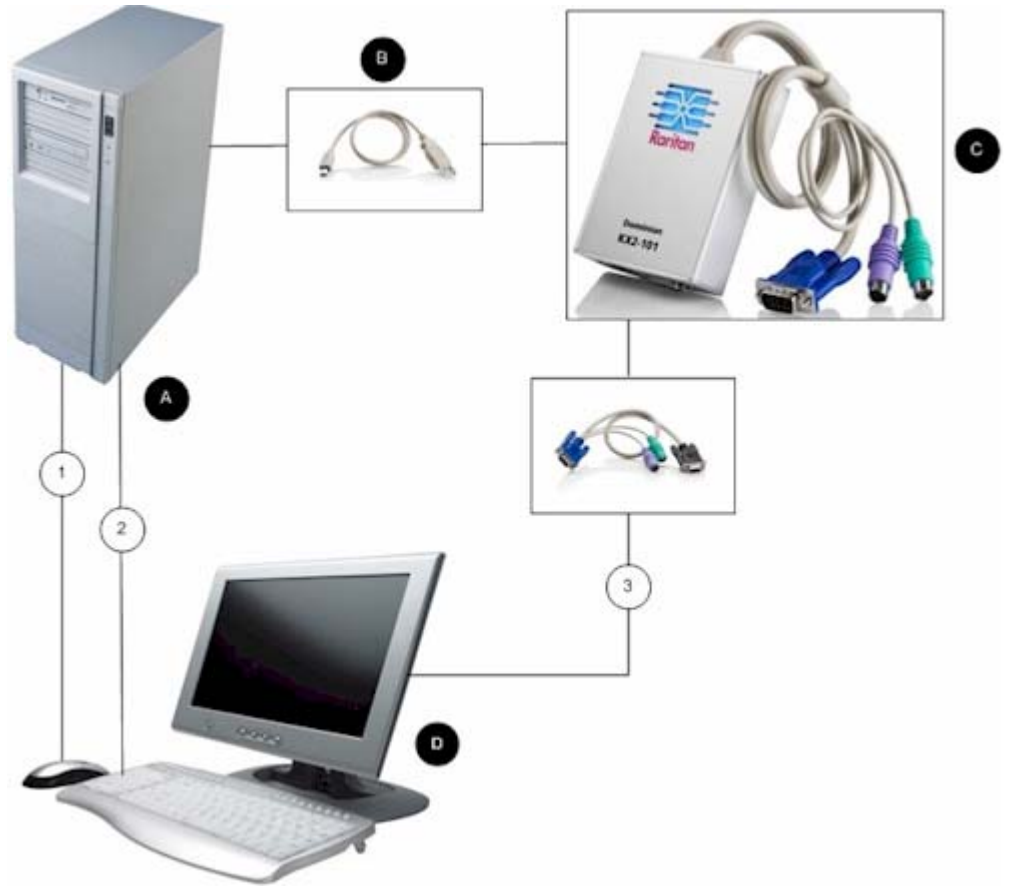


Diagram key

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 (optional cable)

Diagram key	
②	USB connection from the target server to keyboard (optional cable)
③	Video connection to the local monitor (optional cable)

Note: 1, 2 and 3 are required if local access to the target is required.

Note: B also requires an integrated PS2 keyboard, video and mouse cable, with only the video connected.

Note: 1, 2 and 3 are required if local access to the target is required.

Note: B also requires an integrated PS2 keyboard, video and mouse cable, with only the video connected.

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.

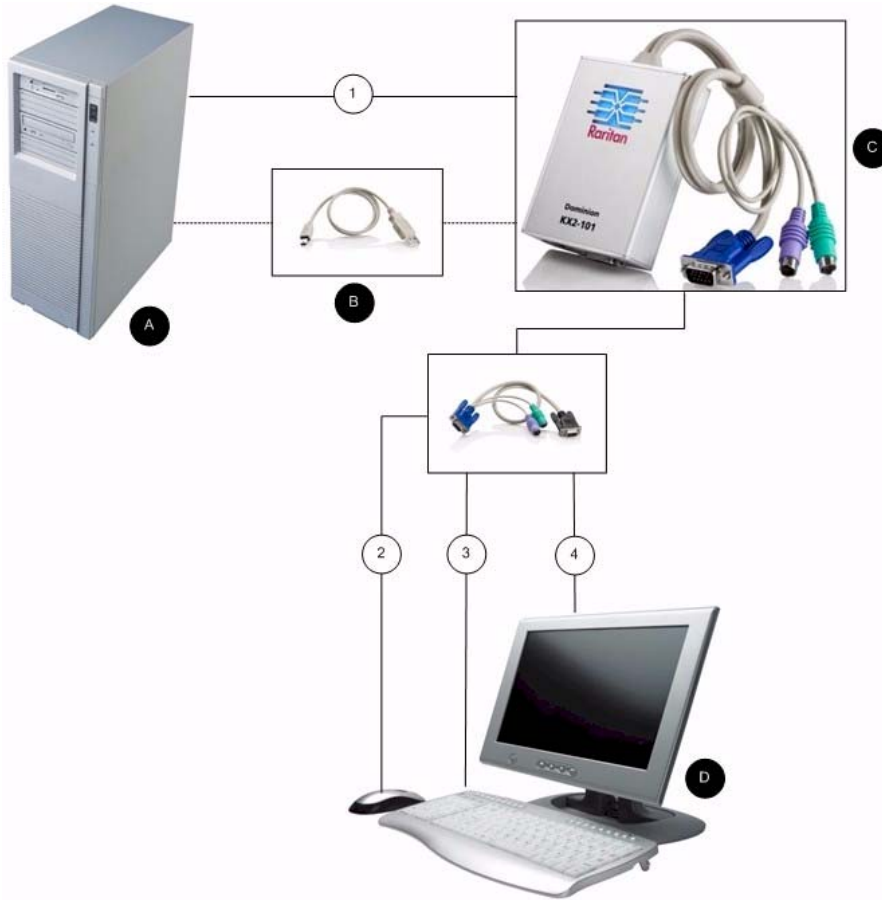


Diagram key

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	
②	PS/2 connection from the KX II-101 to the mouse (optional cable)
③	PS/2 connection from the KX II-101 to the keyboard (optional cable)
④	Video connection to the local monitor (optional cable)

Note: 1, 2 and 3 are required if local access to the target is required.

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

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 28).

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 32 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	Subnet Mask
192.168.59.169	255.255.255.0
Default Gateway	Preferred DHCP Host Name
192.168.59.126	

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 98) 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.

- Click OK.

Home > Device Settings > Port Configuration > Port

Port 1

Type:
KVM

Name:
Dominion_KX2_101_Port1

Power Association

Power Strip Name	Outlet Name
None	---

▶ USB Connection Settings

▶ Advanced USB Connection Settings

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 72) 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

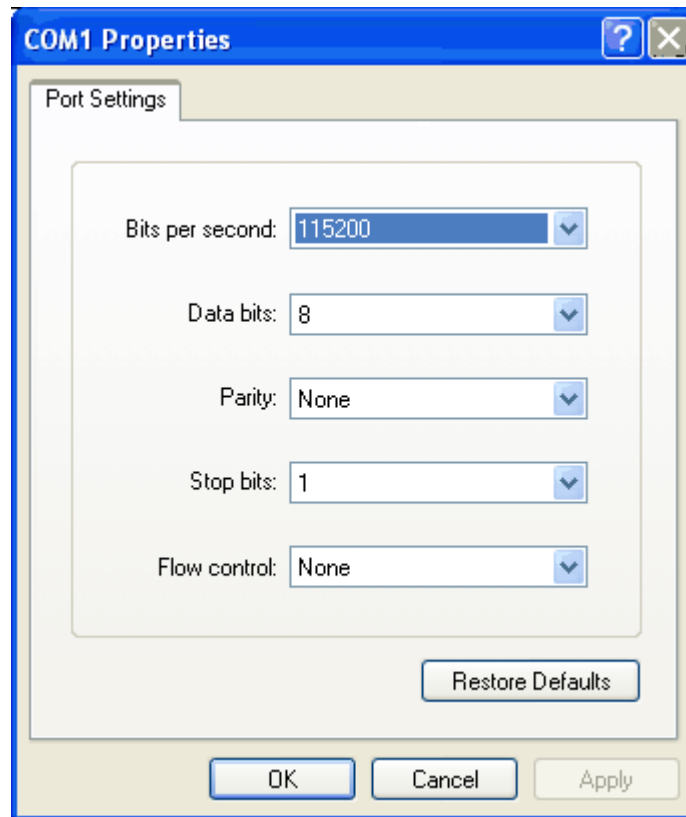
To use a terminal emulation program with the KX II-101, you must first connect the included RS-232 serial cable from the Admin port on the KX II-101 to the COM1 port on your PC. See **Admin Port** (on page 22).

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. If this is the first time you are logging on, you will be prompted to change the admin password.
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.

- 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.
```

- 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	31
Virtual KVM Client	40

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.

The format for a direct port access URL is:

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

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 in to 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** 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 currently available options, depending on the port's status and availability, will be 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 40) 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:**

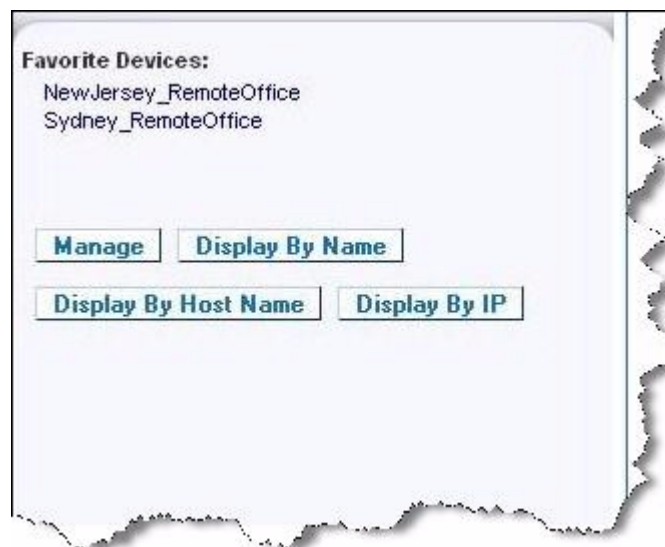
- Click Display by Name.

▶ **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 36).

► **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.

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

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

- Select the checkbox next to the device name/IP address.
- 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.

Home > Manage Favorites > Discover Devices - Local Subnet

Discover Devices - Local Subnet

Use Default Port 5000

Discover on Port:
5000

Save

	Name	IP Address	Host Name
<input type="checkbox"/>	DominionSX	192.168.58.13	
<input type="checkbox"/>	DominionSX	192.168.58.29	
<input type="checkbox"/>	KX2-64	192.168.58.202	

Select All Deselect All

Add Refresh

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 36).

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.

Home > Manage Favorites > Discover Devices - Subnet

Discover Devices - Subnet

	Name	IP Address	Host Name
<input type="checkbox"/>	Neptune	192.168.59.7	
<input type="checkbox"/>	Franklin	192.168.59.8	

Select All Deselect All

Add Refresh

▶ **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.

- 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:**

- From the Favorites List page, select the checkbox next to the appropriate KX II-101 device.
- Click the Edit button. The Edit page appears.
- 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
- Click OK.

► **To delete a favorite:**

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

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

Logging Out

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

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

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

Multi-Platform Client Interface

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

Virtual KVM Client

Overview

Whenever you access a target server using the 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.

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










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 40) window opens to the target server connected to that port.

VKC Toolbar for the KX II-101

Following is a list and description of the standard toolbar buttons in VKC for KX II-101.

Button	Button name	Description
	Connection Properties	Opens the Modify Connection Properties dialog from which you can manually adjust bandwidth options (such as connection speed, color depth, and so forth).
	Video Settings	Opens the Video Settings dialog, allowing you to manually adjust video conversion parameters.
	Synchronize Mouse	In dual-mouse mode, forces realignment of the target server mouse pointer with the mouse pointer.
	Refresh Screen	Forces a refresh of the video screen.
	Auto-sense Video Settings	Forces a refresh of the video settings (resolution, refresh rate).
	Send Ctrl+Alt+Del	Sends a Ctrl+Alt+Del hot key combination to the target server.
	Single Cursor Mode	Starts Single Cursor mode in which the local mouse pointer no longer appears onscreen. Alternatively, press Ctrl+Alt+O to exit single cursor mode.
	Full Screen Mode	Maximizes the screen real estate to view the target server desktop.
	Scaling	Increases or reduces the target video size so you can view the entire contents of the target server window without using the scroll bar.

Power Controlling a KVM Target Server

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

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

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

*Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See **VKC Toolbar for the KX II-101** (on page 41) for additional information.*

► 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 device.
- IP Address - The IP address of the device.
- Port - The KVM communication TCP/IP port used to access the target device.
- Data In/Second - Data rate in.
- Data Out/Second - Data rate out.
- Connect Time - The duration of the connect time.
- FPS - The frames per second transmitted for video.
- Horizontal Resolution - The 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.

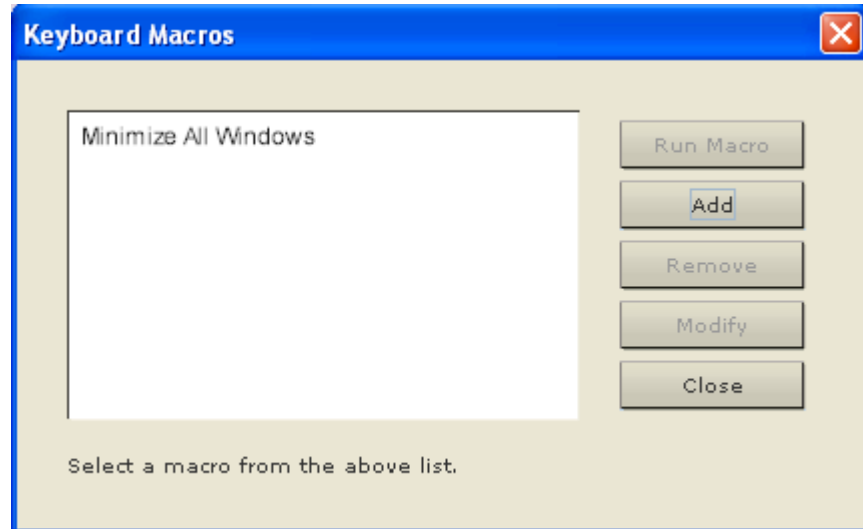
Keyboard macros created in the Virtual KVM Client are available in MPC and vice versa. However, keyboard macros created in AKC cannot be used in VKC or MPC, and vice versa.

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 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, select each key you would like to use to emulate the keystrokes that will be used to perform the command. Select the keys in the order by which they are to be pressed. After each selection, select Add Key. As each key is selected, it will appear in the Macro Sequence field and a Release Key command will automatically be added after each selection.
6. To use the Send Text to Target function for the macro, click the Construct Macro from Text button.
7. For example, create a macro to close a window by selecting Left Ctrl + Esc. This will appear in the Macro Sequence box as follows:
 - Press Left Ctrl
 - Release Left Ctrl
 - Press Esc
 - Release Esc
8. Review the Macro Sequence field to be sure the macro sequence is defined correctly.
 - a. To remove a step in the sequence, select it and click Remove.
 - b. To change the order of steps in the sequence, click the step and then click the up or down arrow buttons to reorder them as needed.
9. 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.

- 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:**

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

Adjusting 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 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.

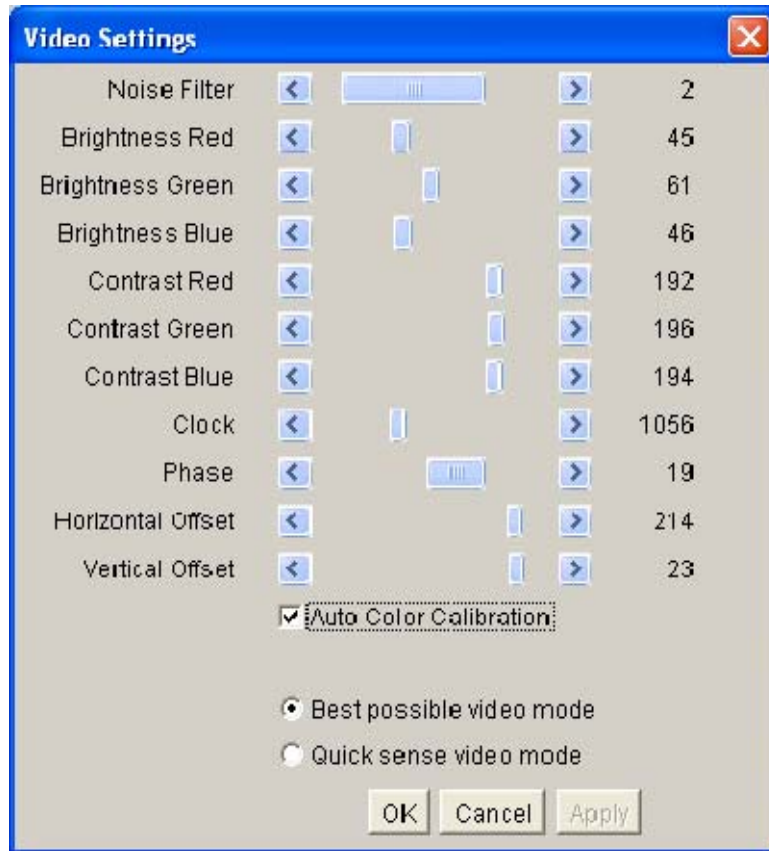
- b. Brightness: Use this setting to adjust the brightness of the target server display.
- c. Brightness Red - Controls the brightness of the target server display for the red signal.
- d. Brightness Green - Controls the brightness of the green signal.
- e. Brightness Blue - Controls the brightness of 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.
 - l. Vertical Offset - Controls the vertical positioning of the target server display on your monitor.
3. Select Auto Color Calibration to enable this feature.
 4. Select the video sensing mode:
 - Best possible video mode
The device will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.
 - Quick sense video mode
With this option, the device will use a quick video Auto Sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.
 5. Click OK to apply the settings and close the dialog. Click Apply to apply the settings without closing the dialog.

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



*Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See **VKC Toolbar for the KX II-101** (on page 41) for additional information.*

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.

*Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See **VKC Toolbar for the KX II-101** (on page 41) for additional information.*

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


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

Auto-Sense Video Settings

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


*Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See **VKC Toolbar for the KX II-101** (on page 41) for additional information.*

► **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.

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.

*Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See **VKC Toolbar for the KX II-101** (on page 41) for additional information.*

Mouse Options

When controlling a target server, the 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 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).

*Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See **VKC Toolbar for the KX II-101** (on page 41) for additional information.*

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 device. The Virtual KVM Client Connection Info dialog displays the actual values that the device 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 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.

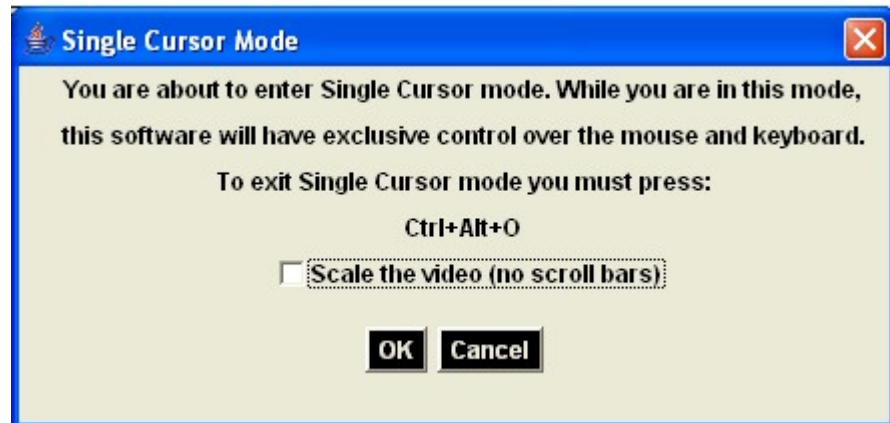
Single Mouse Cursor

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).

*Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See **VKC Toolbar for the KX II-101** (on page 41) for additional information.*

► **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 61) 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 Full Screen 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)
 - Portuguese (Portugal)
 - Danish (Denmark)
 - Swedish (Sweden)
 - German (Switzerland)
 - Hungarian (Hungary)
 - Spanish (Spain)
 - Italian (Italy)
 - Slovenian
 - Translation: French - US
 - Translation: French - US International

Note: In AKC, the keyboard type defaults to the local client, so this option does not apply.

4. Exit Full Screen Mode - Hotkey. When you enter Full Screen mode, the display of the target server becomes full screen and acquires the same resolution as the target server. This is the hot key used for exiting this mode.

Note: The Exit Full Screen Hotkey is not applicable in AKC. In AKC

an Exit Full Screen Mode icon  is displayed instead when you move the mouse to the top of screen.

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. 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)
Portuguese	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 Full Screen mode, the target's full screen is displayed and acquires the same resolution as the target server. The hot key used for exiting this mode is specified in the Options dialog (the default is Ctrl+Alt+M). While in Full Screen mode, moving your mouse to the top of the screen will display the Full Screen mode menu bar.

▶ **To enter full screen mode:**

- Choose View > Full Screen.

▶ **To exit full screen mode:**

- Press the hot key configured in the Tools Options dialog. The default is Ctrl+Alt+M. AKC click the Exit Full Screen mode icon.

Alternatively, if you want to access the target in full screen mode at all times, you can make Full Screen mode the default.

▶ **To set Full Screen mode as the default mode:**

1. Click Tools > Options to open the Options dialog.
2. Select Enable Launch in Full Screen Mode and click OK.

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:**

1. Choose Help > About Raritan Virtual KVM Client.
2. Use the Copy to Clipboard button to copy the information contained in the dialog to a clipboard file so it can be accessed later when dealing with support (if needed).

Chapter 4 Virtual Media

In This Chapter

Overview	62
Prerequisites for Using Virtual Media	65
File Server Setup (File Server ISO Images Only)	66
Using Virtual Media	67
Connecting to Virtual Media	68
Disconnecting Virtual Media	71

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.

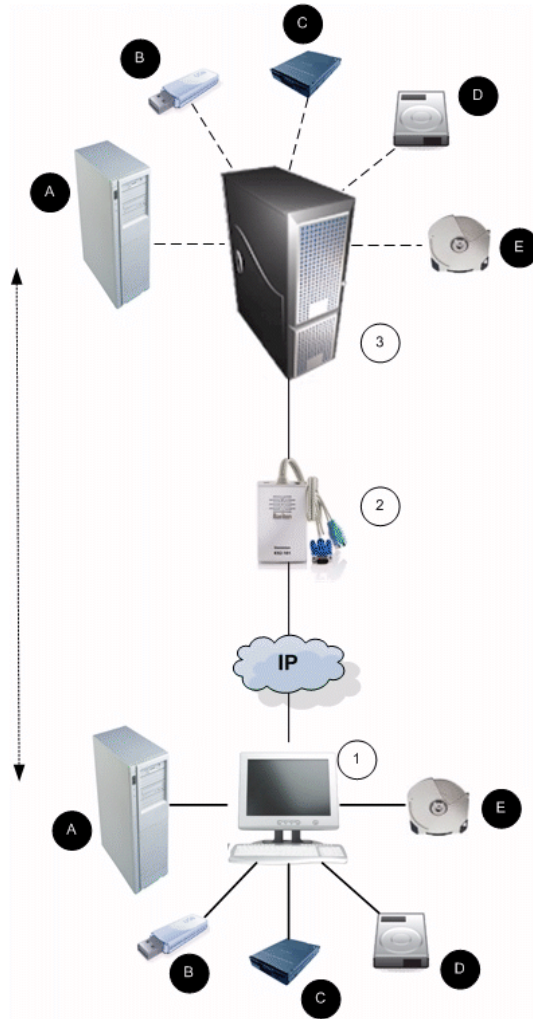


Diagram key	
1	Local workstation
2	KX II-101
3	Target server
A	Remote file server (ISO images)
B	USB drive
C	Floppy drive
D	CD/DVD drive
E	Hard drive image files

Prerequisites for Using Virtual Media

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

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

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

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 or Windows 7, disable User Account Control or select Run as Administrator when starting Internet Explorer. To do this, click the Start Menu, locate IE, right-click and select Run as Administrator.

Target Server

- 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 Remote Console File Server Setup page to designate the files server(s) and image paths that you want to access using virtual media. File server ISO 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**.

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

1. Choose Virtual Media from the Remote Console. The File Server Setup page opens.
2. Check the Selected checkbox for all media that you want accessible as virtual media.
3. Enter information about the file server ISO images that you want to access:
 - IP Address/Host Name - Host name or IP address of the file server.
 - Image Path - Full path name of the location of the ISO image.

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.

Home > File Server Setup Logout

File Server Setup

*IPv4 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	Host Name/IPAddress	Image Path
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Using Virtual Media

See **Prerequisites for Using Virtual Media** (on page 65) before proceeding with using virtual media.

► **To use virtual media:**

1. If you plan to access file server ISO images, identify those file servers and images through the Remote Console File Server Setup page. See **File Server Setup (File Server ISO Images Only)** (on page 66).

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

2. Open a KVM session with the appropriate target server.
 - a. Open the Port Access page from the Remote Console.
 - b. Connect to the target server from the Port Access page:
 - Click the Port Name for the appropriate server.
 - Choose the Connect command from the Port Action menu. The target server opens in a Virtual KVM Client window.
3. Connect to the virtual media.

For:	Select this VM option:
Local drives	Local Drives
Local CD/DVD drives	CD-ROM/DVD-ROM/ISO Images
ISO Images	Connect CD-ROM/ISO Image
File Server ISO Images	Connect CD-ROM/ISO Image

Upon completion of your tasks, disconnect the virtual media. See **Disconnecting Virtual Media** (on page 71).

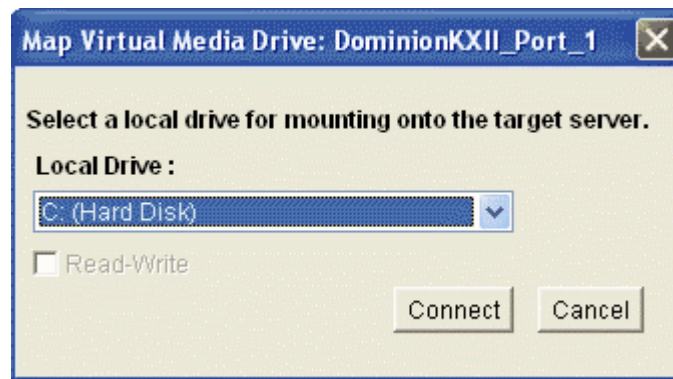
Connecting to Virtual Media

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 69) 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.

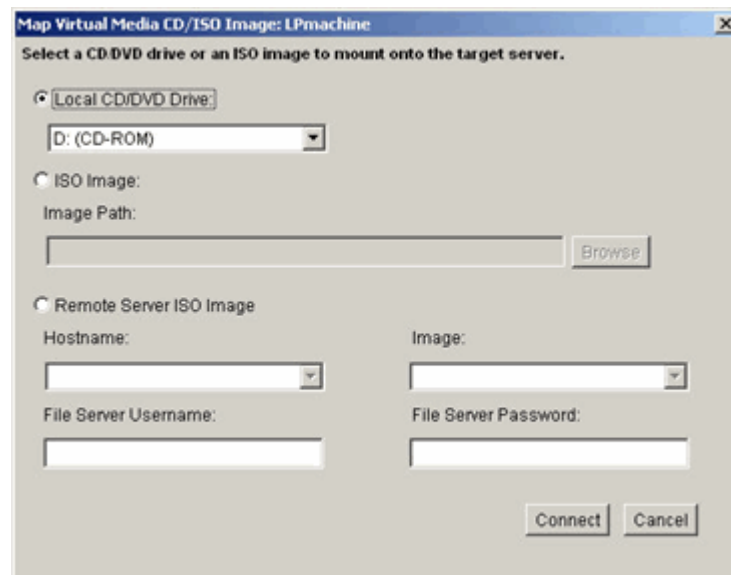
CD-ROM/DVD-ROM/ISO Images

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 list. The file servers and image paths available are those that you configured using the File Server Setup page. Only items you configured using the File Server Setup page will be in the drop-down list.
 - c. File Server Username - User name required for access to the file server.
 - d. File Server Password - Password required for access to the file server (field is masked as you type).
 - e. Click Connect.

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

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

Note: If you are working with Windows 7, Removable Disk is not displayed by default in the Window's My Computer folder when you mount a Local CD/DVD Drive or Local or Remote ISO Image. To view the Local CD/DVD Drive or Local or Remote ISO Image in this folder, select Tools > Folder Options > View and deselect "Hide empty drives in the Computer folder".

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	72
Users	79
Authentication Settings.....	81
Changing a Password	97

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.

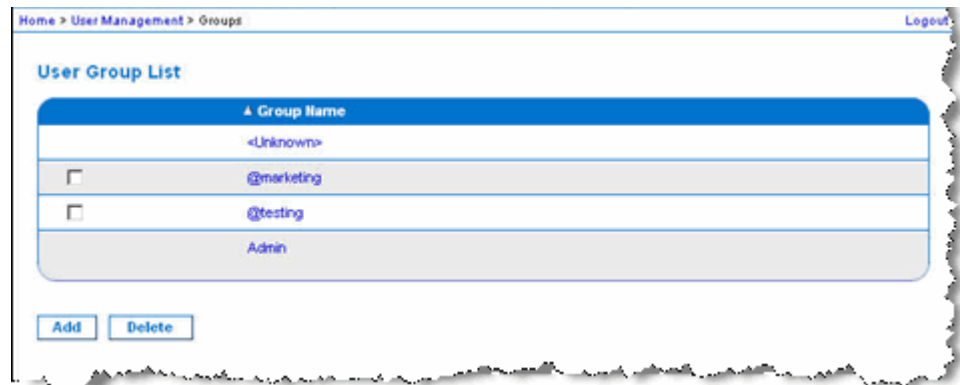
User Group List

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 64 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.

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

*Note: See **Alternate RADIUS Authentication Settings** (on page 88) for information on additional settings if you are using Alternate RADIUS Authentication.*

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.

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

► **To add (append) rules:**

1. Type the starting IP address in the Starting IP field.
2. Type the ending IP address in the Ending IP field.
3. Choose the action from the available options:
 - Accept - IP addresses set to Accept are allowed access to the 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.

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

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

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

*Note: See **Alternate RADIUS Authentication Settings** (on page 88) for information on additional settings if you are using Alternate RADIUS Authentication.*

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

*Note: See **Alternate RADIUS Authentication Settings** (on page 88) for information on additional settings if you are using Alternate RADIUS Authentication.*

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.

*Note: See **Alternate RADIUS Authentication Settings** (on page 88) for information on additional settings if you are using Alternate RADIUS Authentication.*

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 77).
3. Set the Port Permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). See **Setting Port Permissions**.
4. Set the IP ACL (optional). This feature limits access to the KX II-101 device by specifying IP addresses. See **Group-Based IP ACL (Access Control List)**.
5. Click OK.

▶ **To delete a user group:**

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

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

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

Users

Users must be granted user names and passwords to gain access to the 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.



Home > User Management > Users Logout

User List

Username	Full Name	User Group
admin	Admin	Admin
<input type="checkbox"/> marketing	Addie Consumer	@marketing
<input type="checkbox"/> tester	Joe Tester	@tester

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**.

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**.*

► **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 78).

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. Open the User List page by choosing User Management > User List.
2. Locate the user from among those listed on the User List page.
3. Click the user name. The User page opens.
4. On the User page, change the appropriate fields. See **Adding a New User** (on page 80) for information about how to get access the User page.

5. To delete a user, click Delete. You are prompted to confirm the deletion.
6. Click OK.

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 134). 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: When remote authentication (LDAP/LDAPS or RADIUS) is selected, if the user is not found, the local authentication database will also be checked. RADIUS users have the ability to enable Alternate RADIUS Authentication, which accesses the local authentication database only when the remote authentication database is not accessible. See **Implementing RADIUS Remote Authentication** (on page 85).*

► **To configure authentication:**

1. Choose User Management > Authentication Settings. The Authentication Settings page opens.

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

► **To return to factory defaults:**


- Click 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:**

1. Click User Management > Authentication Settings to open the Authentication Settings page.
2. Select the LDAP radio button to enable the LDAP section of the page.
3. Click the  icon to expand the LDAP section of the page.
4. In the Primary LDAP Server field, type the IP address or DNS name of your LDAP/LDAPS remote authentication server (up to 256 characters). When the Enable Secure LDAP option is selected and the Enable LDAPS Server Certificate Validation option is selected, the DNS name must be used to match the CN of LDAP server certificate.
5. In the Secondary LDAP Server field, type the IP address or DNS name of your backup LDAP/LDAPS server (up to 256 characters).

When the Enable Secure LDAP option is selected (see the Enable Secure LDAP step below), the DNS name must be used. Note that the remaining fields share the same settings with the Primary LDAP Server field. **Optional**

6. If you are using a Distinguished Name for the Administrative User, you must enter the password that will be used to authenticate the Administrative User's DN against the remote authentication server. Enter the password in the Secret Phrase field and again in the Confirm Secret Phrase field (up to 128 characters).
7. Select the Enable Secure LDAP checkbox if you would like to use SSL. This will enable the Enable LDAPS Server Certificate Validation checkbox. Secure Sockets Layer (SSL) is a cryptographic protocol that allows 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 only used when the Enable Secure LDAP checkbox is selected.
10. If needed, upload the Root CA Certificate File. This field is enabled when the Enable Secure LDAP option is selected. Consult your authentication server administrator to get the CA certificate file in Base64 encoded X-509 format for the LDAP/LDAPS server. Use the Browse button to navigate to the certificate file. If you are replacing a certificate for the LDAP/LDAPS server with a new certificate, you must reboot the KX II-101 in order for the new certificate to take effect.
11. Enter the Distinguished Name of the Administrative User in the DN of Administrative User field (up to 64 characters). Complete this field if your LDAP server only allows administrators to search user information using the Administrative User role. Consult your authentication server administrator for the appropriate values to type into this field. An example DN of Administrative User value might be *cn=Administrator,cn=Users,dc=testradius,dc=com*. **Optional**
12. In the User Search DN field, enter the Distinguished Name of where in the LDAP database you want to begin searching for user information. Up to 64 characters can be used. An example base search value might be *cn=Users,dc=raritan,dc=com*. Consult your authentication server administrator for the appropriate values to enter into these fields.
13. Select the Type of external LDAP/LDAPS server.
 - Generic LDAP Server.
 - Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.

14. Type the name of the Active Directory Domain. For example, *testradius.com*. Consult your Active Directive Administrator for a specific domain name.
15. Click OK.

The screenshot shows a web interface for 'Authentication Settings'. At the top, there is a breadcrumb trail: 'Home > User Management > Authentication Settings'. Below this is a blue header bar with the text 'Authentication Settings'. Underneath, there are three radio button options: 'Local Authentication', 'LDAP' (which is selected), and 'RADIUS'. A blue bar with a downward arrow and the text 'LDAP' is expanded below these options. The main configuration area includes several fields: 'Primary LDAP Server' and 'Secondary LDAP Server' (both empty text boxes); 'Secret Phrase' and 'Confirm Secret Phrase' (both empty text boxes); an unchecked checkbox for 'Enable Secure LDAP'; 'Port' (text box with '389'); 'Secure LDAP Port' (text box with '636'); 'Certificate File' (text box with a 'Browse...' button); 'DII of Administrative User' (empty text box); 'User Search DII' (empty text box); 'Type of External LDAP Server' (dropdown menu with 'Generic LDAP server' selected); and 'Active Directory Domain' (empty text box).

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 180) 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 82).


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 the RADIUS radio button to enable the RADIUS section of the page.
3. Click the  icon to expand the RADIUS section of the page.
4. In the Primary Radius Server and Secondary Radius Server fields, type the IP address of your primary and optional secondary remote authentication servers, respectively (up to 256 characters).
5. In the Shared Secret fields, type the server secret used for authentication (up to 128 characters).

The shared secret is a character string that must be known by both the KX 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.

11. If you require local authentication to be disabled while the remote authentication database is accessible, select the Alternate RADIUS Authentication checkbox. See **Alternate RADIUS Authentication Settings** (on page 88) and **Alternate RADIUS Authentication Errors** (on page 89) for more information on this feature.

Home > User Management > Authentication Settings

Authentication Settings

Local Authentication
 LDAP
 RADIUS

▶ LDAP

▼ RADIUS

Primary RADIUS Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Secondary RADIUS Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Global Authentication Type
 ▼

Alternate RADIUS Authentication

Alternate RADIUS Authentication Settings

When Alternate RADIUS Authentication is enabled, you are authenticated exclusively against a remote authentication database. If the remote authentication database is inaccessible, you will be authenticated against a local authentication database and will be prompted to enter your local authentication username and password.

Alternate RADIUS Authentication makes use of two user groups: Admin and Operator. Both groups are created automatically and correspond to RADIUS service-type attributes Administrative and Authenticate Only, respectively. Since the local authentication database will be referenced whenever the remote authentication database is inaccessible, the Admin and Operator user groups must consist of users that have been defined locally as members.

Alternate RADIUS Authentication is supported by the Remote Console (**Implementing RADIUS Remote Authentication** (on page 85)), Local Serial Console (**Admin Port** (on page 22)) and SSH Remote Console (**SSH Access when Alternate RADIUS Authentication is Enabled** (on page 159)).

Service-Type Attributes

Access is based on the RADIUS service-type attribute to determine membership in the defined user groups. Valid service-type values and corresponding user groups must be set as follows:

- Administrative = 6 = Admin User Group
- Authenticate Only = 8 = Operator User Group

Permission Settings

The Admin user group is assigned the following permissions settings:

- Device Settings (enabled)
- Diagnostics (enabled)
- Maintenance (enabled)
- PC-Share (enabled)
- Security (enabled)
- User Management (enabled)

The Operator user group has the following by default, but these can be modified by the Admin user.

- Device Settings (disabled)
- Diagnostics (disabled)
- Maintenance (disabled)
- PC-Share (enabled)
- Security (disabled)

- User Management (disabled)

Port Permission Settings

Admin user group has the following Port Permission settings:

- Dominion__KX2_101_Port1 (Access = Control VM Access = Read-Write Power Control = Access)
- Power Port 1 (Access = Control VM Access = Read-Write Power Control = Access)

Operator User Group has the following default Port Permission settings:

- Dominion__KX2_101_Port1 (Access = Control, VM Access = Read-Write, Power Control = Deny)
- Power Port 1 (Access = Deny, VM Access = N/A, Power Control = Deny)

Group Based IP ACL Settings

Admin user group has the following Group-Based IP ACL settings:

- Access for Admin group is always granted.

Operator User Group must have the following default Group-Based IP ACL settings:

- No rules defined.

Alternate RADIUS Authentication Errors

When Alternate RADIUS Authentication is enabled and the remote authentication server is accessible but you cannot be authenticated, you will receive an "Authentication Failed" message.

When the primary authentication server and secondary authentication server (if one is configured) do not respond to an authentication request after the configured request timeout and number of retries, you will receive an "Authentication Timeout" message. You will then be prompted to use your local authentication credentials and the message "Fallback active please login as local username and password" will be displayed.

When fallback is active and local authentication is enabled, if you cannot be authenticated against the local authentication database, the message "Fallback Authentication Failed. Login again and/or default configuration via push-button reset." will be displayed.

Warning: A factory reset will restore all settings on the device to the factory defaults and the device will require reconfiguration.

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

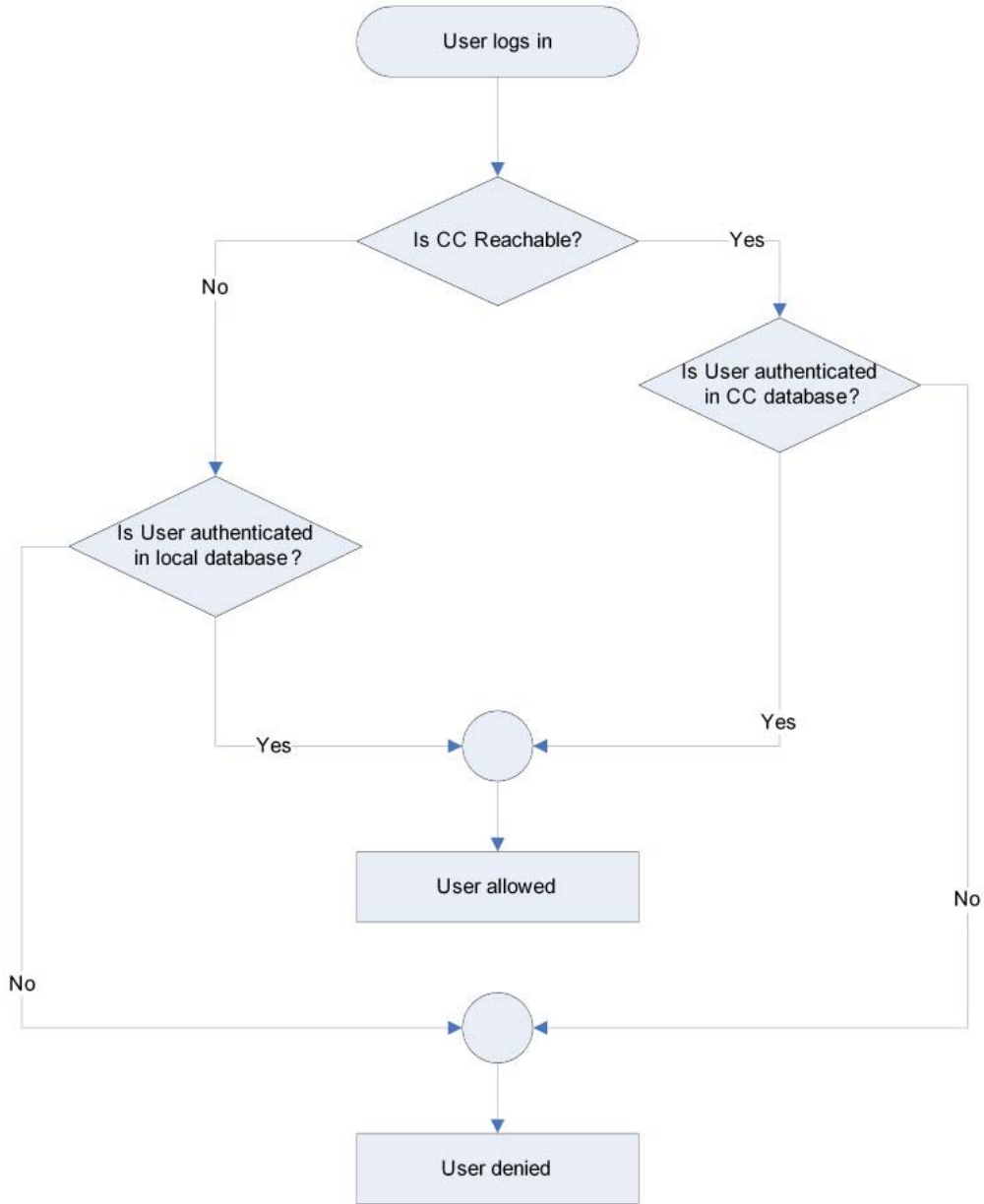
The KX II-101 sends the following RADIUS attributes to your RADIUS server:

Attribute	Data
Log in	
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 out	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - Stops the accounting
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.

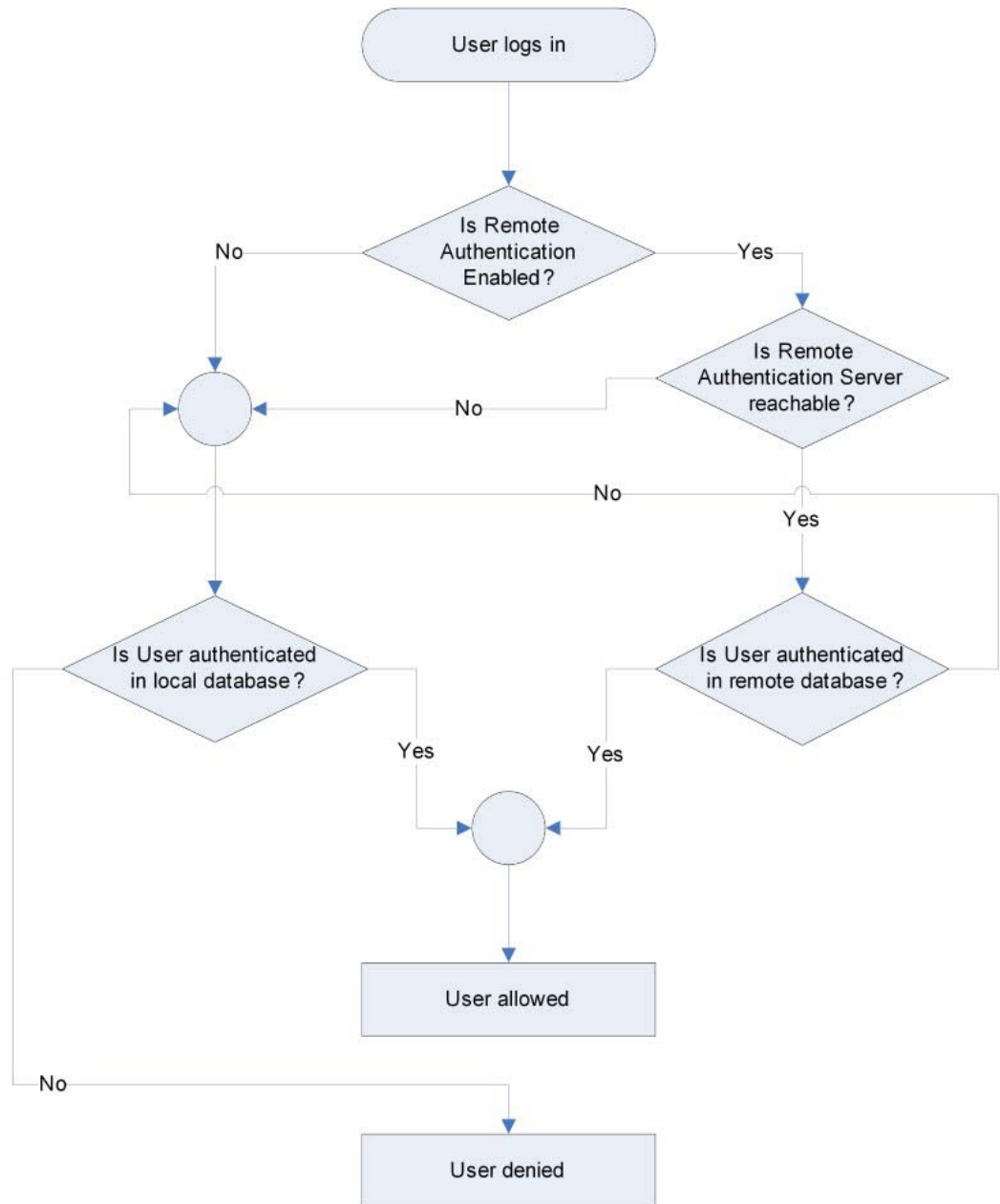
Attribute	Data
Log in	
NAS-IP-Address (4)	The IP address for the KX II-101.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

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:

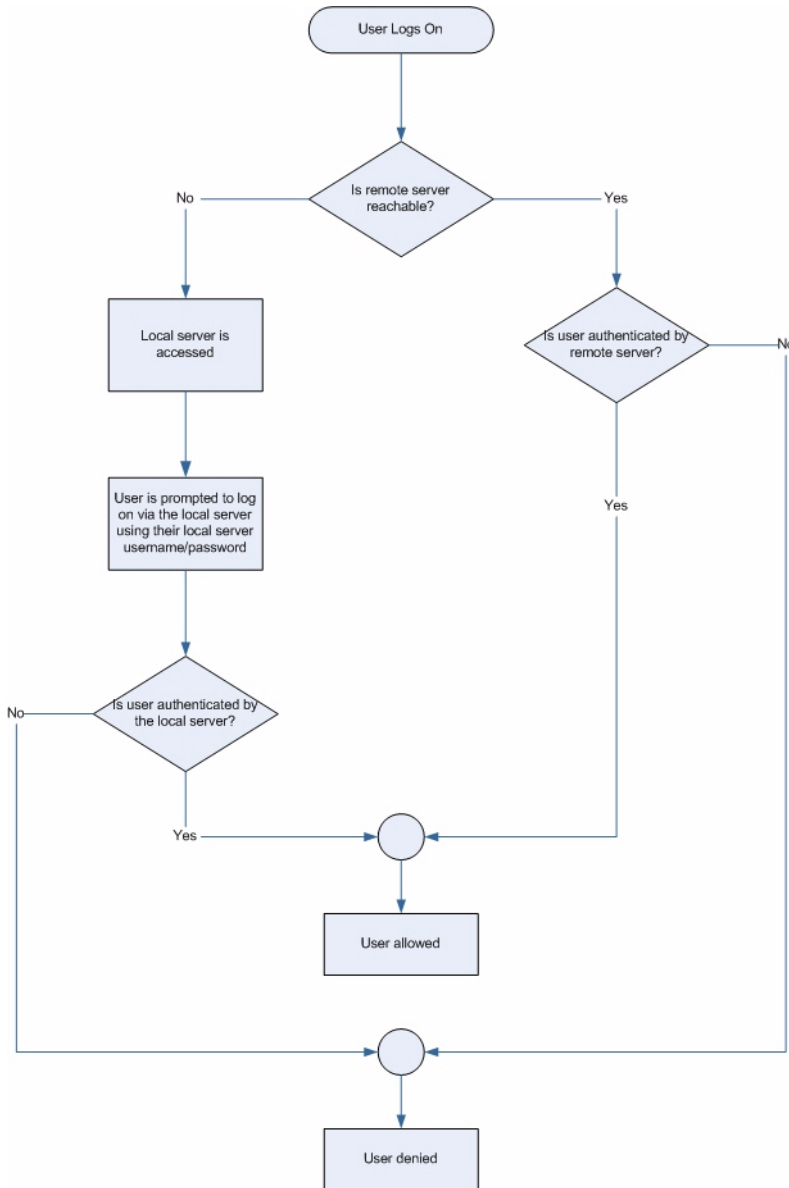


Note: If you are using Alternate RADIUS Authentication, the local authentication process is followed only if the remote authentication server is not reachable.

Alternate RADIUS Authentication

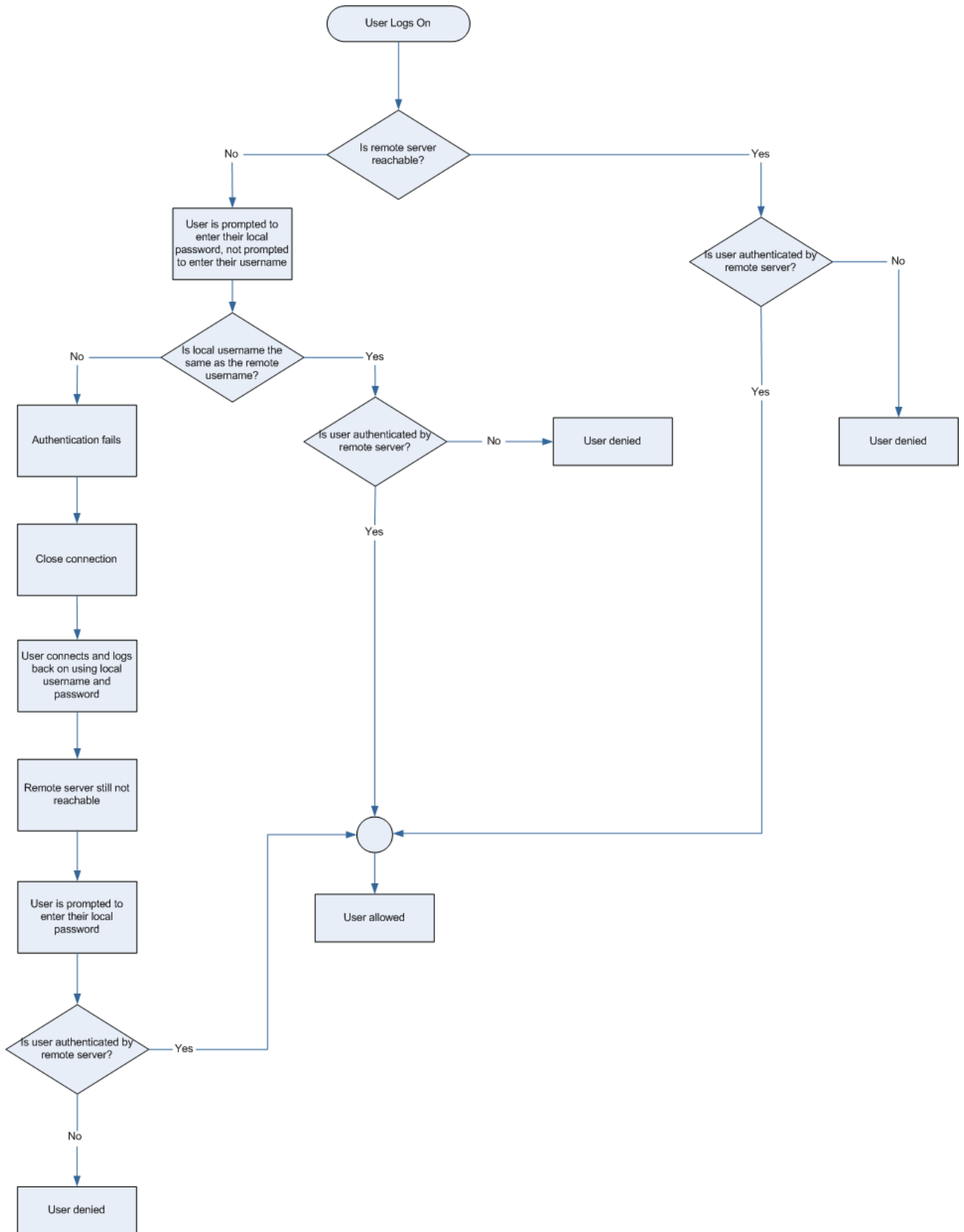
Following are the authentication processes that are followed when using the Admin serial port and MPC, as well as SSH. See **Implementing RADIUS Remote Authentication** (on page 85), **SSH Access when Alternate RADIUS Authentication is Enabled** (on page 159) and **Admin Port** (on page 22).

Admin (Serial) Port and MPC User Authentication Process Flow



Note: When using the Admin serial port and MPC, after three unsuccessful local authentication attempts, fallback mode is deactivated. If you log on successfully with local authentication, fallback mode is deactivated once you log out.

SSH User Authentication Process Flow



Changing a Password

► **To change your password:**

1. Choose User Management > Change Password. The Change Password page opens.
2. Type your current password in the Old Password field.
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 133).*

Home > User Management > Change Password

Change Password

Old Password

New Password

Confirm New Password

Chapter 6 Device Management

In This Chapter

Network Settings	98
Device Services.....	101
Keyboard/Mouse Setup	103
Serial Port Settings.....	104
Date/Time Settings	108
Event Management	109
Port Configuration.....	115
Analog KVM Switch.....	123
Resetting the KX II-101 Using the Reset Button	124

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 99).
3. Update the LAN Interface Settings. See **LAN Interface Settings** (on page 100).
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.

Home > Device Settings > Network Settings

Network Basic Settings	LAN Interface Settings									
<p>Device Name *</p> <input type="text"/>	<p><i>Note: For reliable network communication, configure the Dominion KX2-101 and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX2-101 and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.</i></p> <p>Current LAN interface parameters: autonegotiation on, 100 Mbps, full duplex, link ok</p> <p>LAN Interface Speed & Duplex Autodetect <input type="button" value="v"/></p> <p>Bandwidth Limit No Limit <input type="button" value="v"/></p>									
<p>IP Address</p> <table border="1"> <tr> <td>IP Address</td> <td>Subnet Mask</td> </tr> <tr> <td>192.168.60.17</td> <td>255.255.255.0</td> </tr> <tr> <td>Default Gateway</td> <td>Preferred DHCP Host Name</td> </tr> <tr> <td>192.168.60.126</td> <td><input type="text"/></td> </tr> </table> <p>IP Auto Configuration None <input type="button" value="v"/></p> <p><input type="radio"/> Obtain DNS Server Address Automatically <input type="radio"/> Use the Following DNS Server Addresses</p> <table border="1"> <tr> <td>Primary DNS Server IP Address</td> </tr> <tr> <td>Secondary DNS Server IP Address</td> </tr> </table>		IP Address	Subnet Mask	192.168.60.17	255.255.255.0	Default Gateway	Preferred DHCP Host Name	192.168.60.126	<input type="text"/>	Primary DNS Server IP Address
IP Address	Subnet Mask									
192.168.60.17	255.255.255.0									
Default Gateway	Preferred DHCP Host Name									
192.168.60.126	<input type="text"/>									
Primary DNS Server IP Address										
Secondary DNS Server IP Address										
<p>OK Reset To Defaults Cancel</p>										

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 32 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 maximum 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 177).

- 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 SSH access is enabled by 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.

`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.

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.

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 123).*

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 157).

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 Stop Bits
Data bits Handshake
Parity

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

ATZHD OK ATL0M0&K3X1 OK

Modem server IP address

192.168.3.1

Modem client IP address

192.168.3.2

See **Modem Access Cable Connections** (on page 108) for details on the cable connection for modem access and see **Certified Modems** (on page 175) 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** in the **KVM and Serial Clients Guide**.

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**

- Click OK.

Home > Device Settings > Date/Time Settings

Date/Time Settings

Time Zone
 (GMT -05:00) US Eastern ▼

Adjust for daylight saving time

User Specified Time

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

Time (Hour, Minute)
 10 : 18

Synchronize with NTP Server

Primary Time server

Secondary Time server

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 110).*

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

1. Choose Device Settings > Event Management - Destinations. The Event Management - Destinations page opens.
System events are categorized by Device Operation, Device Management, Security, User Activity, and User Group Administration.
2. Select the checkboxes for those event line items you want to enable or disable, and where you want to send the information.

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

3. Click OK.

Home > Device Settings > Event Management - Destinations Logout

Event Management - Destinations

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

Category	Event	SNMP	Syslog	Audit Log
Device Operation		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Startup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	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"/>
	Ethernet Failover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Management		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	FactoryReset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Begin CC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	End CC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Started	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Completed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	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"/>
	Port Connection Denied	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security		<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 Blocked		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Activity		<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"/>

► **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
bladeChassisCommError	A communications error with blade chassis device connected to this port was detected. <i>Note: Not supported by the KX II-101.</i>
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.
ipConflictResolved	An IP Address conflict was resolved.

Trap Name	Description
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.
userForcedLogout	A user was forcibly logged out by Admin
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.
userUploadedCertificate	A user uploaded a SSL certificate.
vmlImageConnected	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.
vmlImageDisconnected	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.

No.	Name	Type
1	Dominion_KX2_101_Port1	KVM
2	Power Port 1	PowerStrip

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

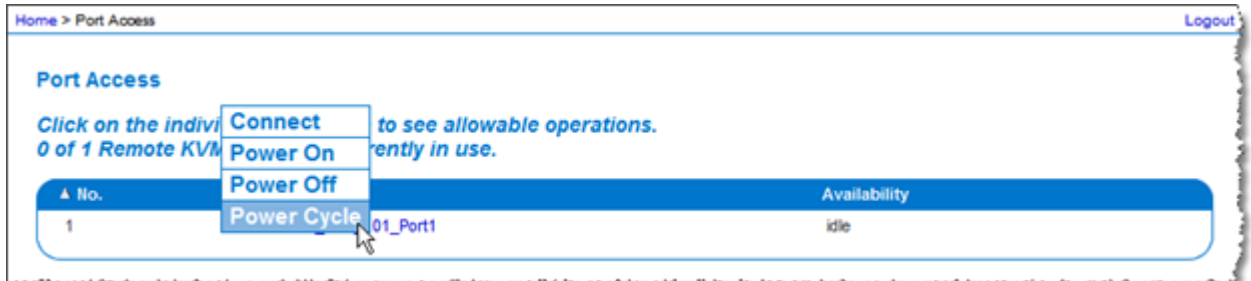
- Click the Port Name for the port you want to edit.
 - For KVM ports, the Port page is opened. In this page, you can name the ports, create power associations, and set target server settings.
 - For power strips, the Port page for power strips is opened. In this page, you can name the power strips and their outlets. See **Power Control** (on page 118).

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 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 118).*

► **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:

- 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.

- 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 118).
- 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 119).
- Associate outlet in the power strip to the target server. See **Managing KVM Target Servers (Port Page)** (on page 116).
- Turn the outlets on the power strip on and off in the Power Strip Device page. See **Controlling a Power Strip Device** (on page 122).

Connecting the Power Strip

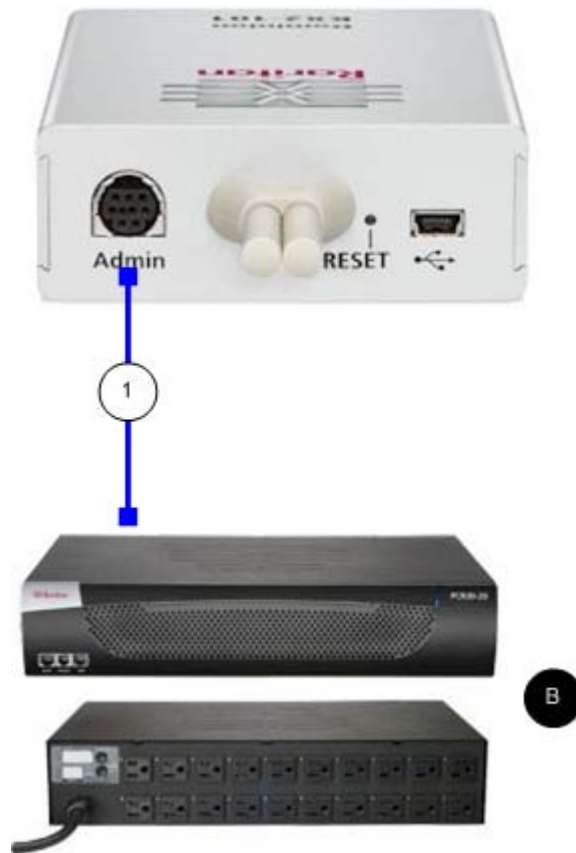




Diagram key	
	DKX2-101-SPDUC connector (not included) from the KX II-101 to Raritan the power strip.
	Raritan power strip.

► **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).

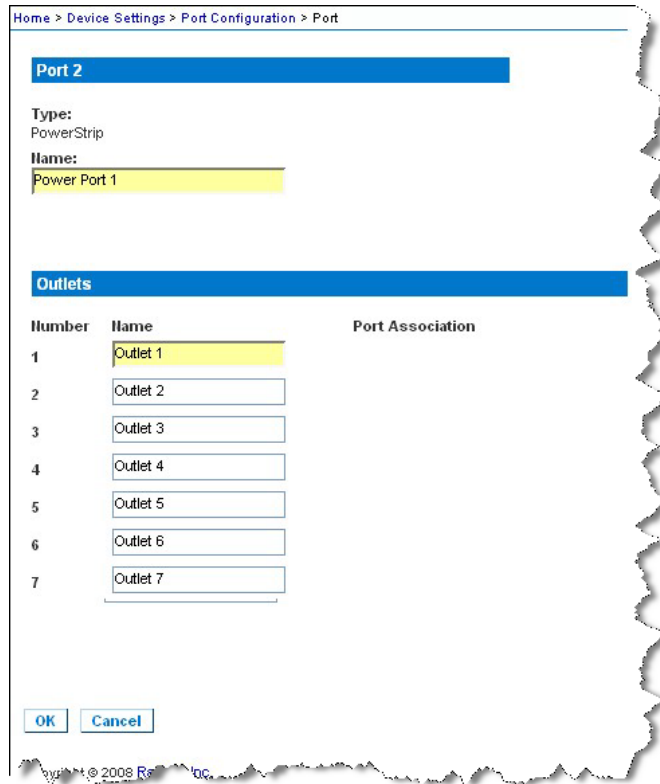
► **To name the power strip (and outlets):**

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.



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:**

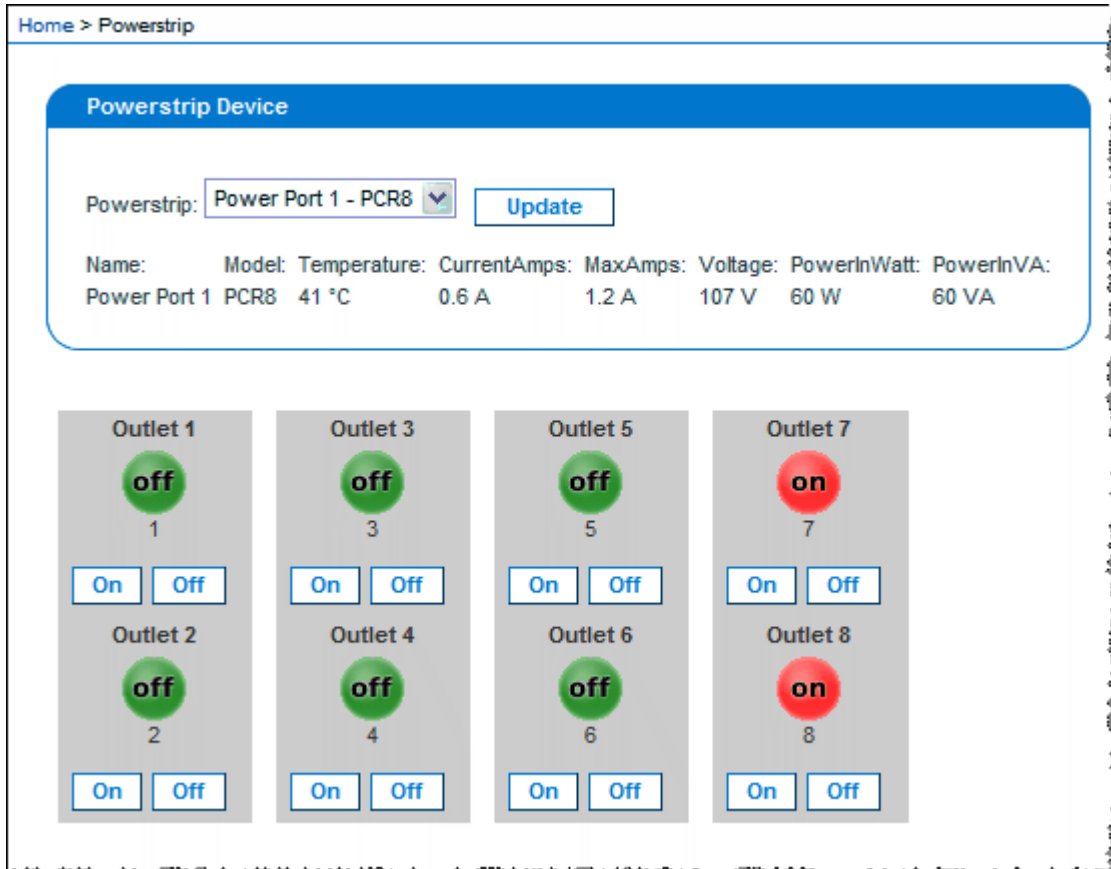
- Choose Home > Device Settings > Port Configuration > [power port name]. The outlet associations for the power strip appear under Outlets.

▶ **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 122).
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.



► **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:

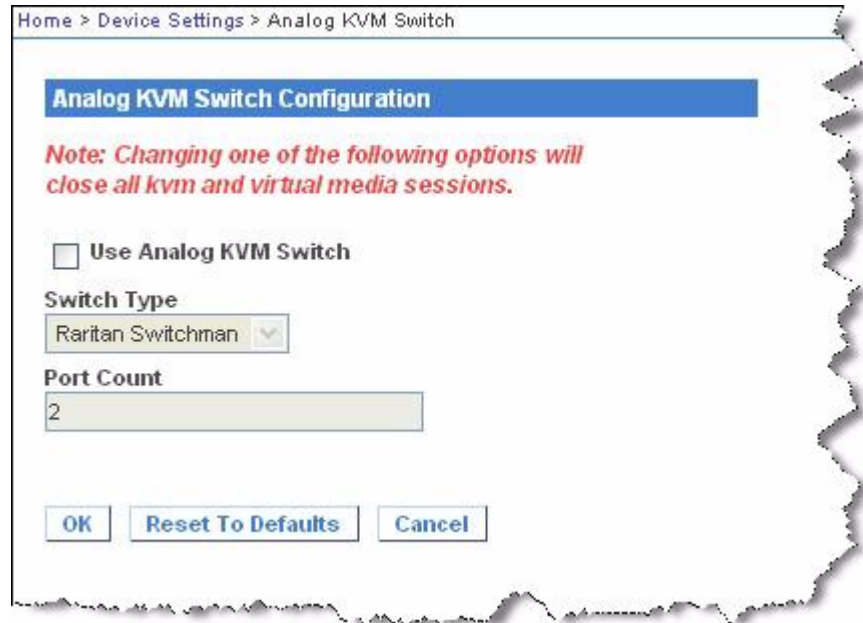
1. Set the Host Interface on the Keyboard/Mouse Setup page to PS/2. If you don't do this and try to configure an analog KVM switch, you will receive the error "PS/2 is needed to access the KVM Switch. Please enable PS/2 first!" on the Analog KVM Switch Configuration page. See **Keyboard/Mouse Setup** (on page 103).
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

6. 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

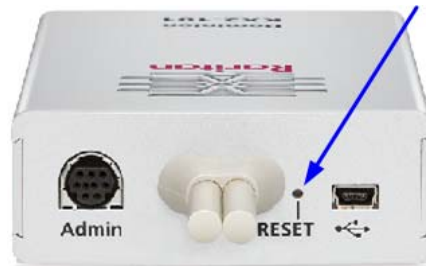
On the back panel of the device, there is a Reset button. It is recessed to prevent accidental resets (you will need a pointed object to press this button).

The actions that are performed when the Reset button is pressed are defined in the graphical user interface. See **Encryption & Share** (on page 135).

► **To reset the device:**

1. Power off the KX II-101.
2. Use a pointed object to press and hold the Reset button.
3. While continuing to hold the Reset button, power the KX II-101 device back on.
4. Continue holding the Reset button for 10 seconds.
5. 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.....	127
Basic USB Connection Settings	127
Advanced USB Connection Settings.....	129

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.

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.

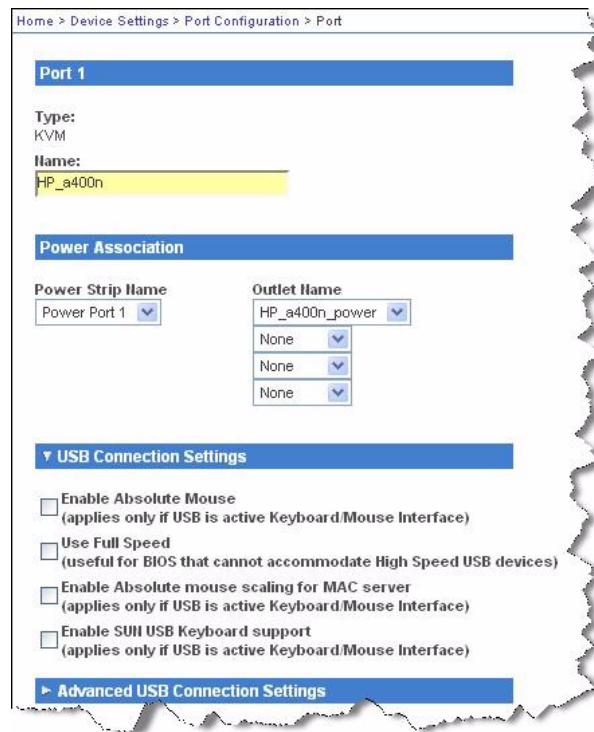
Should none of the USB Connection settings provided by Raritan work with a given KVM target, please contact Raritan Technical Support for assistance.

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 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	Outlet Name
Power Port 1	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

Chapter 8 Security Management

In This Chapter

Security Settings.....	131
IP Access Control	139

Security Settings

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

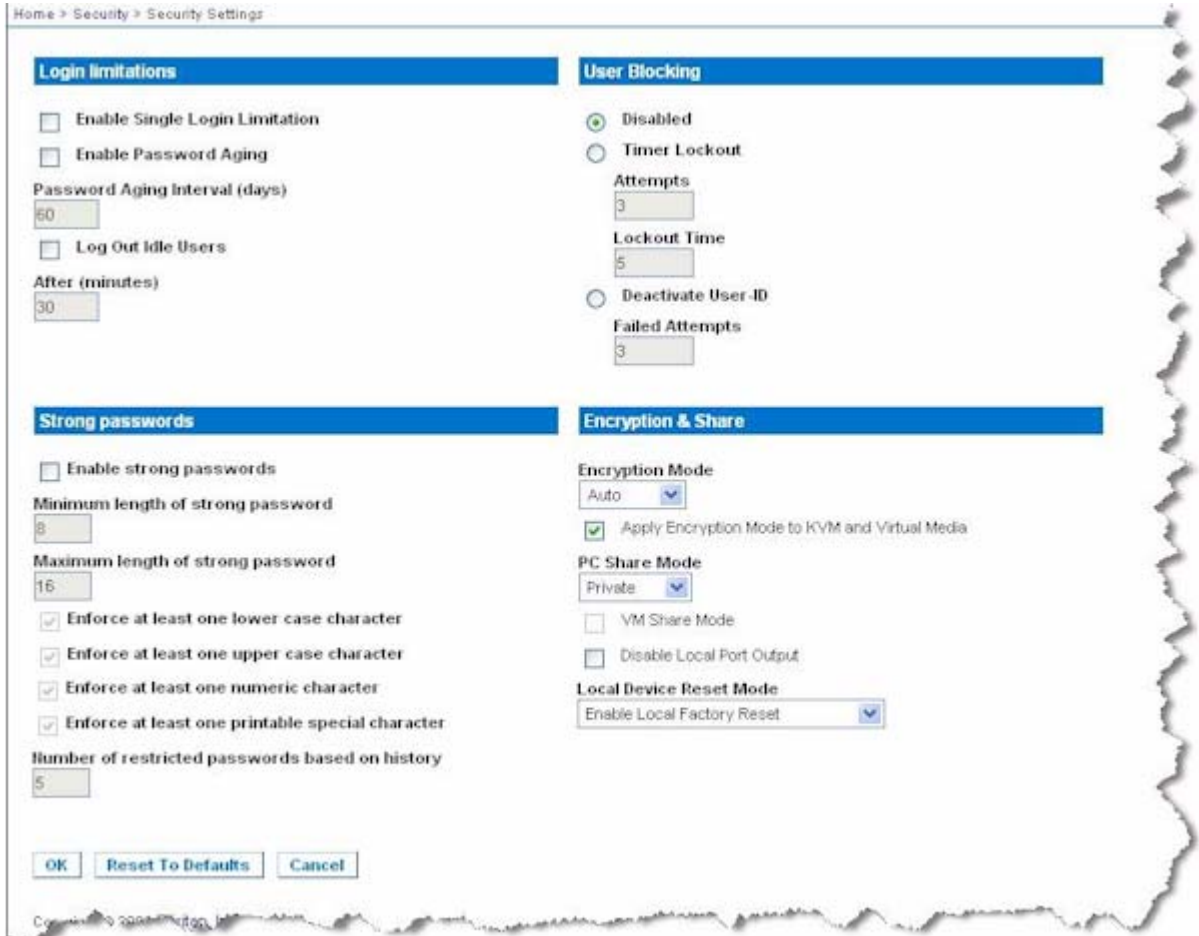
Raritan SSL certificates are used for public and private key exchanges, and provide an additional level of security. Raritan web server certificates are self-signed. Java applet certificates are signed by a VeriSign certificate. Encryption guarantees that your information is safe from eavesdropping and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

► **To configure the security settings:**

1. Choose Security > Security Settings. The Security Settings page opens.
2. Update the **Login Limitations** (on page 132) settings as appropriate.
3. Update the **Strong Passwords** (on page 133) settings as appropriate.
4. Update the **User Blocking** (on page 134) settings as appropriate.
5. Update the **Encryption & Share** (on page 135) settings as appropriate.
6. Click OK.

► **To reset back to defaults:**

- Click Reset to Defaults.



Login Limitations

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

Limitation	Description
Enable single login limitation	When selected, only one login per user name is allowed at any time. When deselected, a given user name/password combination can be connected into the device from several client workstations simultaneously.
Enable password aging	When selected, all users are required to change their passwords periodically based on the

Limitation	Description
	<p>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 out idle users, After (1-365 minutes)	<p>Select the "Log off idle users" checkbox to automatically disconnect users after the amount of time you specify in the "After (1-365 minutes)" field. If there is no activity from the keyboard or mouse, all sessions and all resources are logged out. If a virtual media session is in progress, however, the session does not timeout.</p> <p>The After field is used to set the amount of time (in minutes) after which an idle user will be logged out. This field is enabled when the Log Out Idle Users option is selected. Up to 365 minutes can be entered as the field value</p>

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 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	When checked, at least one lower case

Field	Description
case character	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 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. <hr/> <p><i>Note: Users in the role of Administrator are exempt from the timer lockout settings.</i></p>
Deactivate User-ID	<p>When selected, this option specifies that the user will be locked out of the system after the number of failed login attempts specified in the Failed Attempts field:</p> <ul style="list-style-type: none"> ▪ Failed Attempts - The number of unsuccessful login attempts after which the user's User-ID will be deactivated. This field is enabled when the Deactivate User-ID option is selected. The valid range is 1 - 10.

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.

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 KX II-101."

Encryption mode	Description
Auto	This is the recommended option. The KX II-101 autonegotiates to the highest level of encryption possible. You <i>must</i> select Auto in order for the device and client to successfully negotiate the use of FIPS compliant algorithms. See also FIPS Support Requirements (see "FIPS 140-2 Support Requirements" on page 138).
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.
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 138) 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 138) 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.

- 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. This setting applies only to the KX2 832 and KX2 864. If you are using smart card readers, the local port *must* be disabled.
6. If needed, select Local Device Reset Mode. This option specifies which actions are taken when the hardware Reset button (at the back of the device) is depressed. For more information, see ***Resetting the KX II-101 Using the Reset Button*** (on page 124). Choose one of the following options:

Local device reset 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 and 3
- Mozilla 1.7.13
- Internet Explorer 7 and 8

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

FIPS 140-2 Support Requirements

The KX II-101 supports the use of FIPS 140-20 approved encryption algorithms. This allows an SSL server and client to successfully negotiate the cipher suite used for the encrypted session when a client is configured for FIPS 140-2 only mode.

Following are the recommendations for using FIPS 140-2 with the KX II-101:

KX II-101

- Set the Encryption & Share to Auto on the Security Settings page. See **Encryption & Share** (on page 135).

Microsoft Client

- FIPS 140-2 should be enabled on the client computer and in Internet Explorer.

► To enable FIPS 140-2 on a Windows client:

1. Select Control Panel > Administrative Tools > Local Security Policy to open the Local Security Settings dialog.
2. From the navigation tree, select Select Local Policies > Security Options.

3. Enable "System Cryptography: Use FIPS compliant algorithms for encryption, hashing and signing".
4. Reboot the client computer.

▶ **To enable FIPS 140-2 in Internet Explorer:**

1. In Internet Explorer, select Tools > Internet Options and click on the Advanced tab.
2. Select the Use TLS 1.0 checkbox.
3. Restart the browser.

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.

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, CIDR notation consists of two parts. The most significant part is the network address, which identifies a whole network or subnet. The least significant portion is the identifier. The prefix length after the / identifies the length of the subnet mask.

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

To allow access to only one IP address and block all others, change the subnet mask for the rule to /32. For example, if you are trying to exclude all access from the '192.168.51' subnet and the Default Policy is Accept, you would Append a Rule with IP/MASK set to 192.168.51.00/24 and a policy DROP. Or, if you are trying to exclude all access from the 192.168.51 subnet except from a specific IP address (192.168.51.105) and the Default Policy is Accept, you would:

1. Append Rule 1 with IP/Mask set to 192.168.51.105/32 and a policy of Accept.
2. Append Rule 2 with IP/Mask set to 192.168.51.0/24 and a policy of Drop.

If you reversed Rule 1 and Rule 2, 192.168.51.105 would also not be able to access the KX II-101 since it would also have been dropped by the first rule that is encountered.

Chapter 9 Maintenance

In This Chapter

Audit Log.....	142
Device Information.....	143
Backup and Restore	144
Upgrading Firmware	146
Upgrade History.....	148
Factory Reset	148
Rebooting	149

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:**

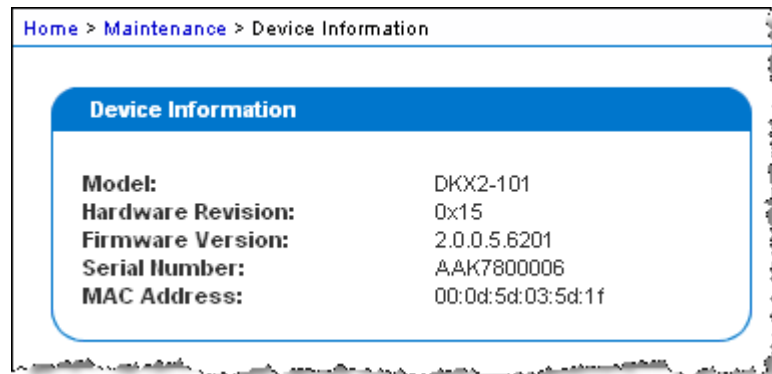
- Use the [Older] and [Newer] links.

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.

Home > Maintenance > Backup / Restore

Backup / Restore

Full Restore
 Protected Restore
 Custom Restore

User and Group Restore
 Device Settings Restore

Restore File

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

► **If you are using Firefox or Internet Explorer 5 or lower, 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.

► **If you are using Internet Explorer 6 or higher, to backup your KX II-101:**

1. Click Backup. A File Download dialog appears that contains an Open button. Do not click Open.

In IE 6 and higher, IE is used as the default application to open files, so you are prompted to open the file versus save the file. To avoid this, you must change the default application that is used to open files to Wordpad.

2. To do this:
 - a. Save the backup file. The backup file is saved locally on your client machine with the name and location specified.
 - b. Once saved, locate the file and right-click on it. Select properties.
 - c. In general tab, click Change and select Wordpad.

► **To restore your 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:
 - User and Group Restore - This option includes only user and group information. This option *does not* restore the certificate and the private key files. Use this option to quickly set up users on a different KX II-101.
 - Device Settings Restore - This option includes only device settings such as power associations, USB profiles, blade chassis related configuration parameters, and Port Group assignments. Use this option to quickly copy the device information.
1. Click Browse. A Choose File dialog appears.

2. Navigate to and select the appropriate backup file and click Open. The selected file is listed in the Restore File field.
3. Click Restore. The configuration (based on the type of restore selected) is restored.

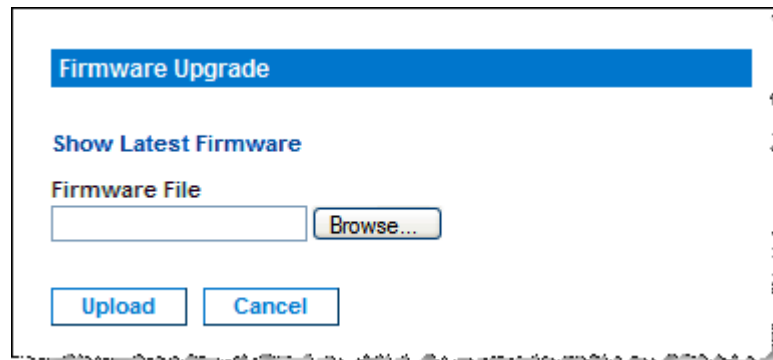
Upgrading Firmware

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:**

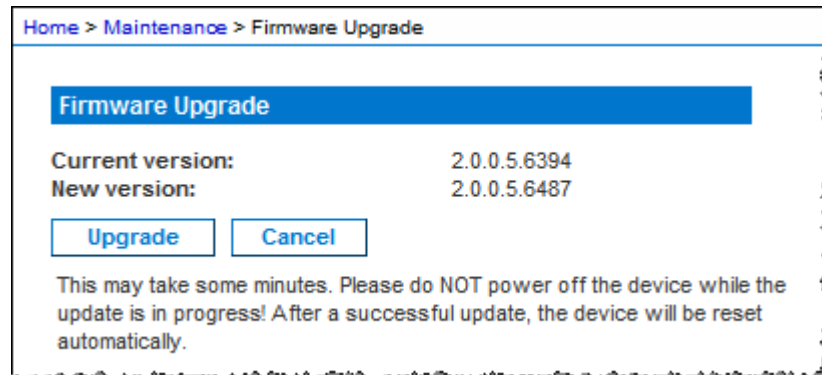
1. Choose Maintenance > Firmware Upgrade. The Firmware Upgrade page opens.



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.

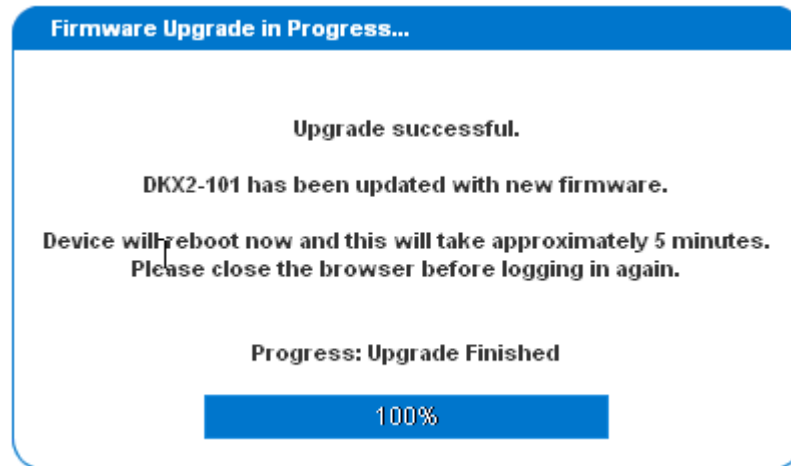
Note: Copy the firmware update file to a local PC before uploading. Do not load the file from a network drive. Click the Browse button to navigate to the directory where you unzipped the upgrade file.

- Click Upload from the Firmware Upgrade page. Information about the upgrade and version numbers is displayed for your confirmation:



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.

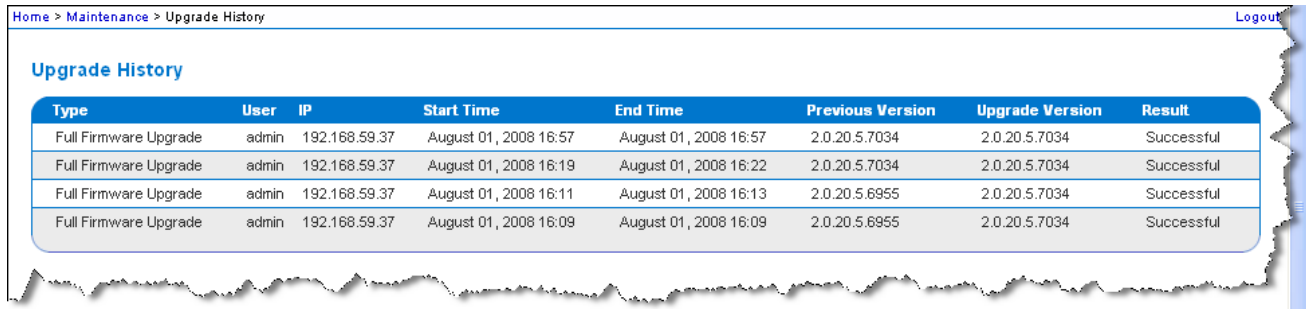
For information about upgrading the device firmware using the Multi-Platform Client, see the **Raritan Multi-Platform Client (MPC) User Guide**.

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

Factory Reset

*Note: It is recommended that you save the audit log prior to performing a factory reset. The audit log is deleted when a factory reset is performed and the reset event is not logged in the audit log. For more information about saving the audit log, see **Audit Log**.*

► **To perform a factory reset:**

1. Choose Maintenance > Factory Reset. The Factory Reset page opens.
2. Choose the appropriate reset option from the following options:
 - Full Factory Reset - Removes the entire configuration and resets the device completely to the factory defaults. Note that any management associations with CommandCenter will be broken. Because of the complete nature of this reset, you will be prompted to confirm the factory reset.
 - Network Parameter Reset - Resets the network parameters of the device back to the default values (click Device Settings > Network Settings to access this information):
 - IP auto configuration
 - IP address
 - Subnet mask
 - Gateway IP address

- Primary DNS server IP address
 - Secondary DNS server IP address
 - Discovery port
 - Bandwidth limit
 - LAN interface speed & duplex
 - Enable automatic failover
 - Ping interval (seconds)
 - Timeout (seconds)
1. Click Reset to continue. You will be prompted to confirm the factory reset because all network settings will be permanently lost.
 2. Click OK button proceed. Upon completion, the KX II-101 device is automatically restarted.

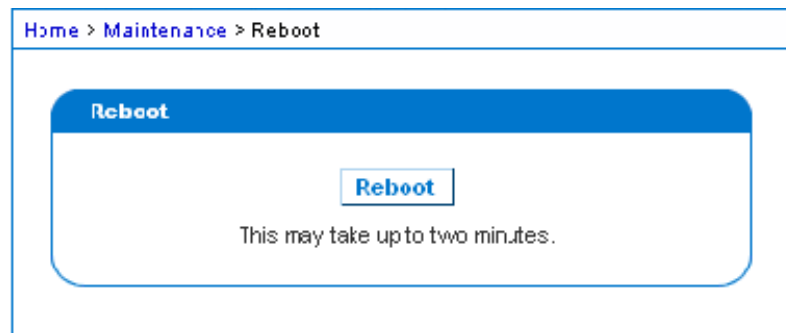
Rebooting

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	151
Network Statistics Page.....	151
Ping Host Page.....	153
Trace Route to Host Page.....	154
Device Diagnostics	155

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.

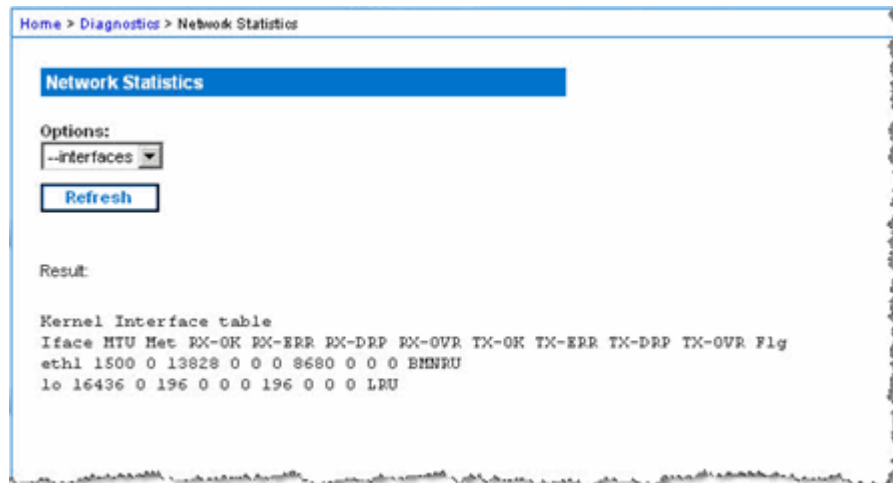
► **To view statistics about your network interface:**

1. Choose Diagnostics > Network Statistics. The Network Statistics page opens.
2. Choose the appropriate option from the Options drop-down list:

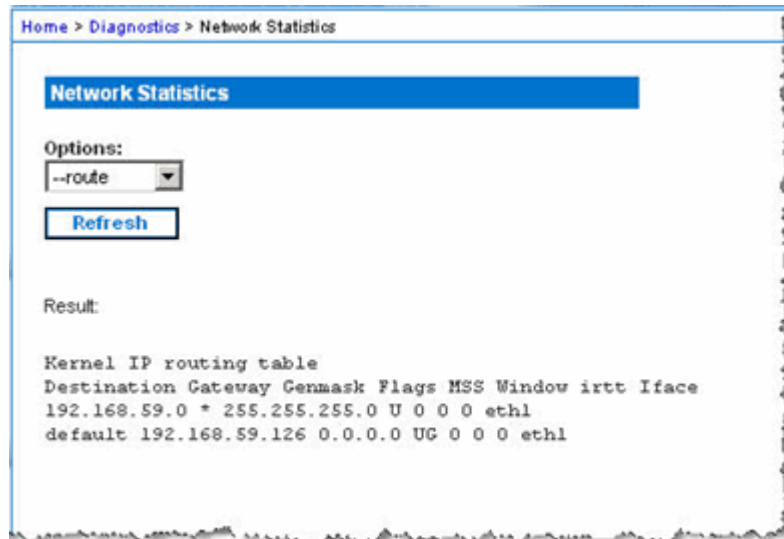
- Statistics - Produces a page similar to the one displayed here.



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



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



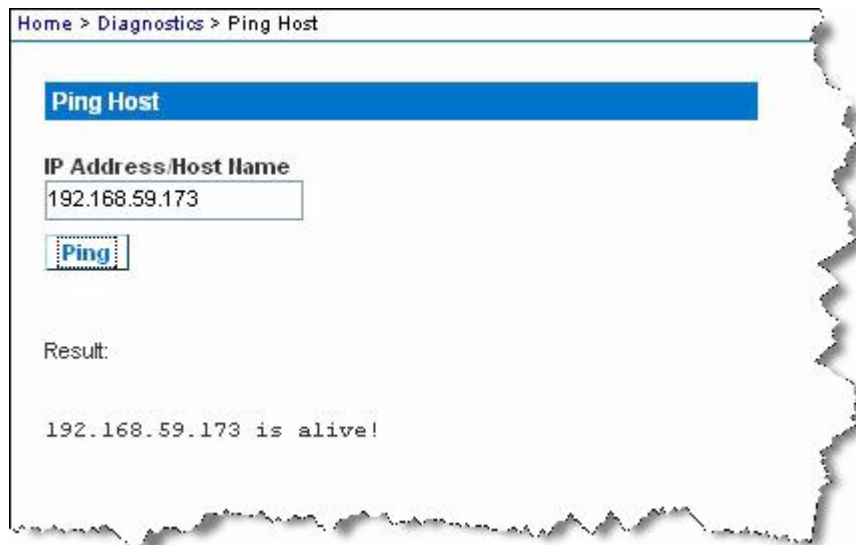
3. Click Refresh. The relevant information is displayed in the Result field.

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

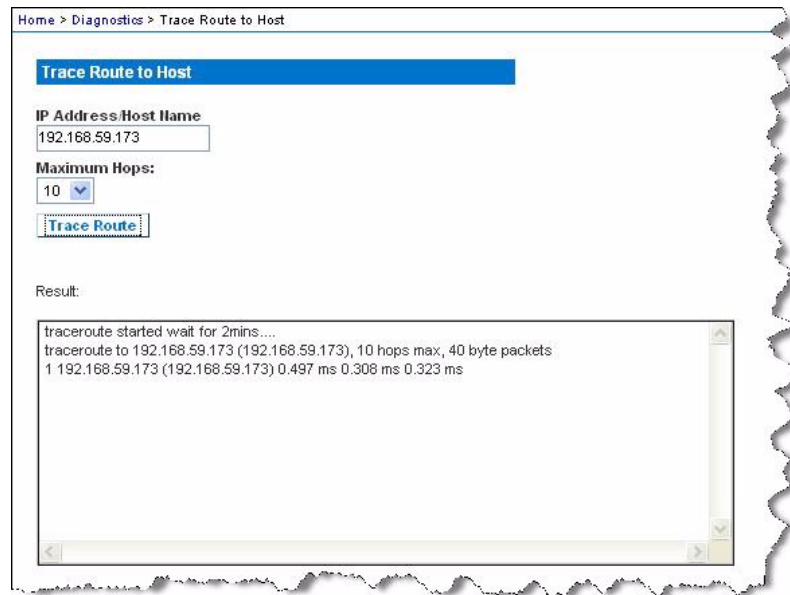
Trace route is a network tool used to determine the route taken to the provided hostname or IP address.

► **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.



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.

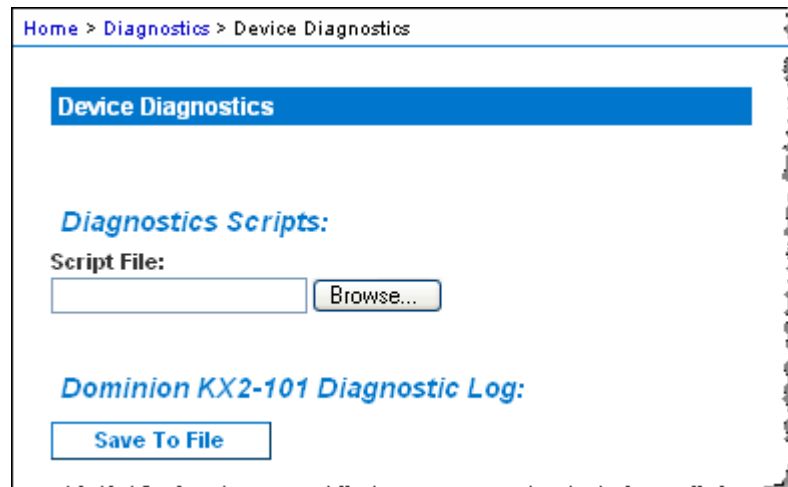
Use the following settings:

- 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.

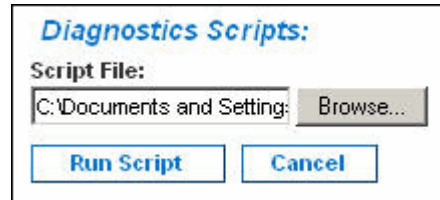
► To run the KX II-101 System diagnostics:

1. Choose Diagnostics > Device Diagnostics. The Device Diagnostics page opens.

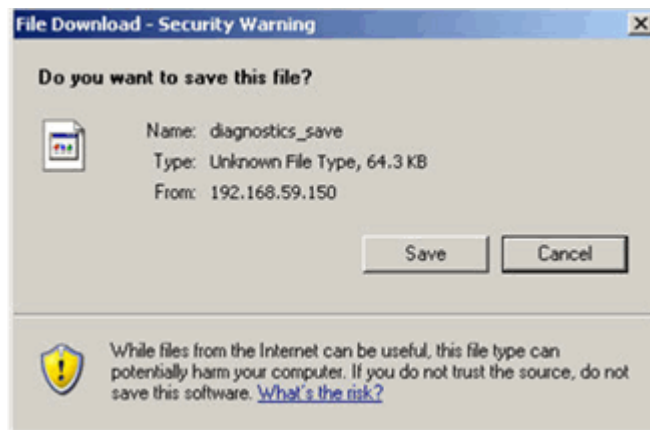


2. (Optional) Perform the following steps if you have received a diagnostics script file from Raritan Technical Support. Otherwise, skip to step 3.
 - a. Retrieve the diagnostics file supplied by Raritan and unzip as necessary.

- 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)

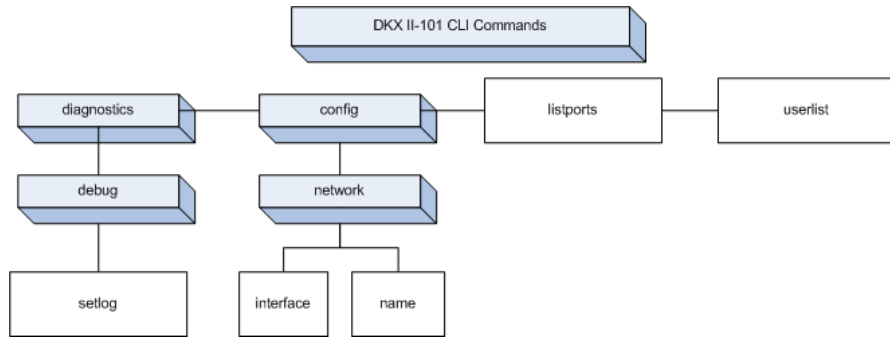
In This Chapter

Overview.....	157
Accessing the KX II-101 Using the CLI	158
SSH Connection to the KX II-101	158
Logging On	159
Navigation of the CLI	160
CLI Commands.....	162

Overview

This chapter provides an overview of the CLI commands that can be used with the KX II-101. See **CLI Commands** (on page 162) 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 101).*

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 101).

Note: For security reasons, SSH V1 connections are not supported by the KX II-101.

SSH Access from a Windows PC (Shared KSX II, KX II 101, SX)

► **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.

The login as: prompt appears.

SSH Access from a UNIX/Linux Workstation

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

```
ssh -l admin 192.168.30.222
```

The Password prompt appears.

SSH Access when Alternate RADIUS Authentication is Enabled

When Alternate RADIUS Authentication is enabled, you are authenticated exclusively against a remote authentication database. If the remote authentication database is inaccessible, you will be authenticated against a local authentication database and will be prompted to enter your local authentication username and password. When this happens, the following information and prompts will be displayed:

```
Authentication Timeout
Fallback active please login as local username and password
```

See **User Authentication Process** (on page 92) for details on the authentication process flow for SSH when Alternate RADIUS Authentication is enabled.

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 160) section, you can perform the initial configuration tasks described in **Configure the KX II-101 Using a Terminal Emulation Program (Optional)** (on page 28).

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 >
```

0

Completion of Commands

The CLI supports the completion of partially-entered commands. After entering the first few characters of an entry, press the Tab key. If the characters form a unique match, the CLI will complete the entry.

- If no match is found, the CLI displays the valid entries for that level.
- If multiple matches are found, the CLI displays all valid entries.

Enter additional text to make the entry unique and press the Tab key to complete the entry.

CLI Syntax -Tips and Shortcuts

Tips

- Commands are listed in alphabetical order.
- Commands are not case sensitive.
- Parameter names are single word without underscore.
- Commands without arguments default to show current settings for the command.
- Typing a question mark (?) after a command produces help for that command.
- A pipe symbol (|) indicates a choice within an optional or required set of keywords or arguments.

Shortcuts

- Press the Up arrow key to display the last entry.
- Press Backspace to delete the last character typed.
- Press Ctrl + C to terminate a command or cancel a command if you typed the wrong parameters.
- Press Enter to execute the command.
- Press Tab to complete a command. For example, `Admin Port > Conf.` The system then displays the `Admin Port > Config >` prompt.

Common Commands for All Command Line Interface Levels

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.

Command	Description
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	Switch to the diagnostics menu. See Diagnostics (on page 163).
debug	Switch to debug menu. See Debug (on page 163).
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	Lists the port, port name, port type, port status, and port availability. See Listports Command (on page 166).
logout	Logout of the current CLI session.
name	Sets the device name. See Name Command (on page 164).
network	Displays network configuration and enables you to configure network settings. See Network (on page 164).
quit	Return to previous command.
setlog	Sets device logging options. See Setlog Command (on page 163).
top	Return to the root menu.
userlist	Lists the number of active users, user names, port, and status. See Userlist Command (on page 166).

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

Command Option	Description
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 8).

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
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.....	167
Removing a KX II-101 from CC-SG Management	168
Using CC-SG in Proxy Mode.....	169

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.

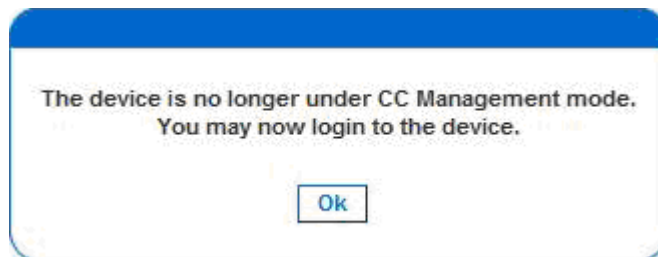


► **To remove the device from CC-SG management (to use CC Unmanage):**

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	170
Supported Video Resolutions	171
Supported Keyboard Languages	172
Supported Operating Systems (Clients)	173
Supported Browsers	175
Certified Modems	175
Connectors	175
TCP and UDP Ports Used	175
Network Speed Settings	177
Admin Port Pinout Information	178
9 Pin Pinout	178

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 <ul style="list-style-type: none"> ▪ 100-240V~/ 6VDC +/- 3% ▪ Maximum current rating: 1.3A @ 6V • Power over Ethernet (PoE) <ul style="list-style-type: none"> ▪ Mid-Span Power Insertion ▪ Signal-Pair Power Insertion ▪ Voltage rating for PoE standard: 36V - 57V ▪ Maximum current rating: 0.16A @ 48V
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 /

Specification	Description
	mouse and virtual media connectivity to the target <ul style="list-style-type: none"> 1- MiniDIN9 port for multi-function serial port of full RS-232 features, modem connection, and Dominion PX connectivity
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	1152x900 @76 Hz

Resolutions		
	Hz	
640x480 @85 Hz	832x624 @75.1 Hz	1280x960 @60 Hz
640x480 @90 Hz	1024x768 @60 Hz	1280x960 @85 Hz
640x480 @100 Hz	1024x768 @70 Hz	1280x1024 @60 Hz
640x480 @120 Hz	1024x768 @72 Hz	1280x1024 @75 Hz
720x400 @70 Hz	1024x768 @75 Hz	1280x1024 @85 Hz
720x400 @84 Hz	1024x768 @85 Hz	1600x1200 @60 Hz

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

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 Hanguk
Japanese	Japan	JIS Keyboard
French	France	French (AZERTY)

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

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 7®	Yes
Windows XP®	Yes
Windows 2008®	Yes
Windows Vista®	Yes
Windows 2000 SP4® Server	Yes
Windows 2003® Server	Yes
Windows 2008® Server	Yes
Red Hat® Desktop 5.0	Yes. Locally held ISO image, Remote File Server mounting directly from KX II-101.
Red Hat Desktop 4.0	Yes. Locally held ISO image, Remote File Server mounting directly from KX II-101.
Open SUSE 10, 11	Yes. Locally held ISO image, Remote File Server mounting directly from KX

Client OS	Virtual media (VM) support on client
	II-101.
Fedora™ 8 - 11	Yes. Locally held ISO image, Remote File Server mounting directly from KX II-101.
Mac OS	No
Solaris	No

The JRE plug-in is available for the Windows 32-bit and 64-bit operating systems. MPC and VKC can be launched only from a 32-bit browser, or 64-bit IE7 or IE8 browser.

Following are the Java 32-bit and 64-bit Windows operating system requirements.

Mode	Operating system	Browser
Windows x64 32-bit mode	Windows XP	<ul style="list-style-type: none"> • IE 6.0 SP1+ or 7.0, IE 8 • Mozilla 1.4.X or 1.7+ • Netscape 7.X • Firefox 1.06 - 3
	Windows Server 2003	<ul style="list-style-type: none"> • IE 6.0 SP1++, IE 7, IE 8 • Mozilla 1.4.X or 1.7+ • Netscape 7.X • Firefox 1.06 - 3
	Windows Vista	<ul style="list-style-type: none"> • IE 7.0 or 8.0
	Windows 7	<ul style="list-style-type: none"> • IE 7.0 or 8.0 • Firefox 1.06 - 3
Windows x64 64-bit mode	Windows XP	64bit OS, 32bit browsers:
	Windows XP Professional	<ul style="list-style-type: none"> • IE 6.0 SP1+, 7.0 or 8.0 • Mozilla 1.4.X or 1.7+
	Windows XP Tablet	<ul style="list-style-type: none"> • Netscape 7.X
	Windows Vista	<ul style="list-style-type: none"> • Firefox 1.06 - 3
	Windows Server 2003	64bit mode, 64bit browsers:
	Windows Server 2008	<ul style="list-style-type: none"> • IE 7.0 or 8.0
	Windows 7	

Supported Browsers

KX II-101 supports the following browsers:

- Internet Explorer 6, 7 and 8
- Firefox 1.5, 2.0, and 3.0 (up to build 3.0.10)
- 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

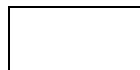
TCP and UDP Ports Used

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/VKC) 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 98).
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 logons 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 logons 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 logons 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
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

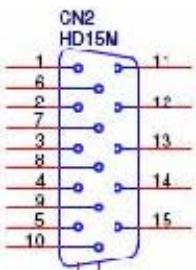
communication,” however, note that the KX II-101 behavior deviates from expected behavior

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	180
Setting the Registry to Permit Write Operations to the Schema	181
Creating a New Attribute	181
Adding Attributes to the Class	182
Updating the Schema Cache.....	184
Editing rcusergroup Attributes for User Members	184

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:

rcusergroup 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.

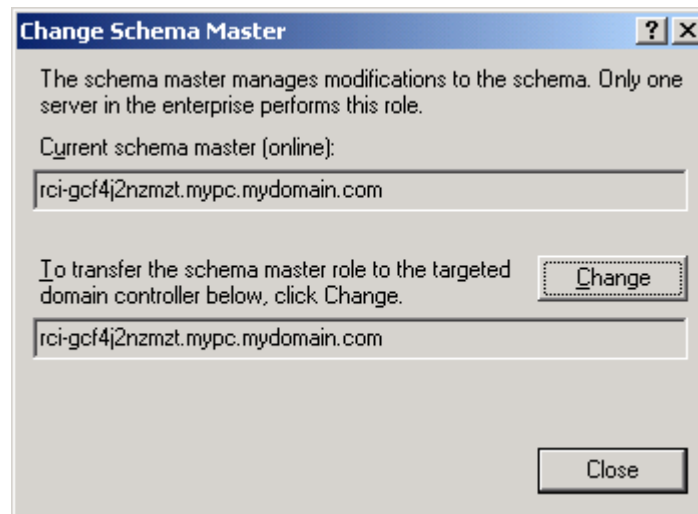
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

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.

3. Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.

Create New Attribute

Create a New Attribute Object

Identification

Common Name: rciusergroup

LDAP Display Name: rciusergroup

Unique X500 Object ID: 1.3.6.1.4.1.13742.50

Description: Raritan's LDAP attribute

Syntax and Range

Syntax: Case Insensitive String

Minimum: 1

Maximum: 24

Multi-Valued

OK Cancel

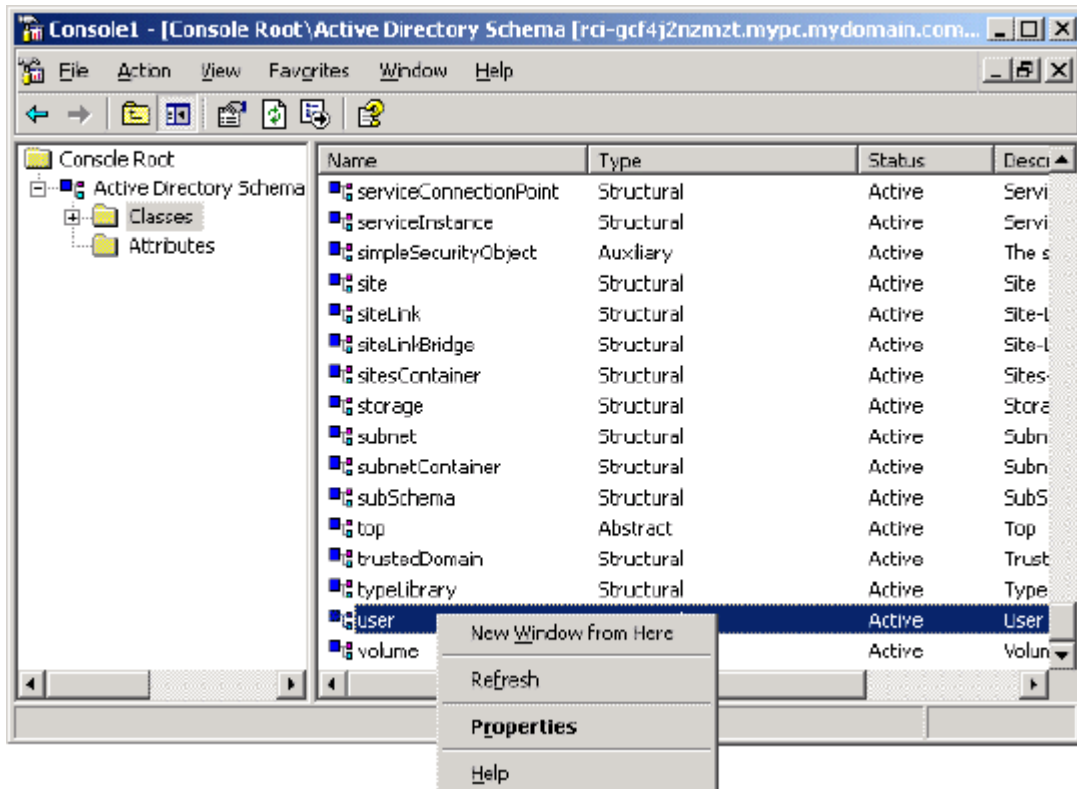
4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
9. Type *1* in the Minimum field.
10. Type *24* in the Maximum field.
11. Click OK to create the new attribute.

Adding Attributes to the Class

► **To add attributes to the class:**

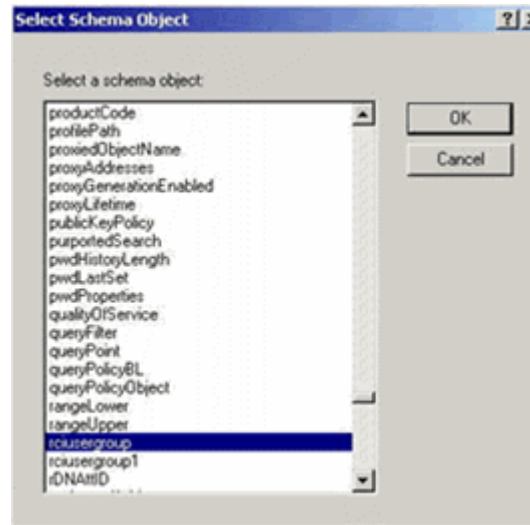
1. Click Classes in the left pane of the window.

2. Scroll to the user class in the right pane and right-click it.



3. Choose Properties from the menu. The user Properties dialog appears.
4. Click the Attributes tab to open it.
5. Click Add.

6. Choose rciusergroup from the Select Schema Object list.



7. Click OK in the Select Schema Object dialog.
8. Click OK in the User Properties dialog.

Updating the Schema Cache

► **To update the schema cache:**

1. Right-click Active Directory Schema in the left pane of the window and select Reload the Schema.
2. Minimize the Active Directory Schema MMC (Microsoft Management Console) console.

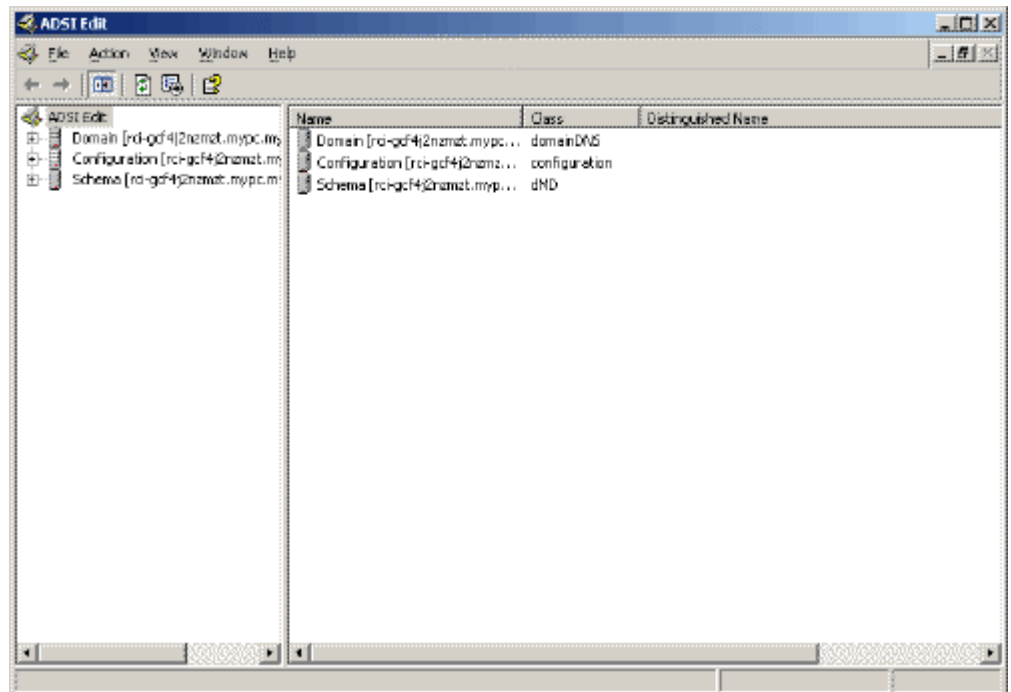
Editing rciusergroup Attributes for User Members

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.

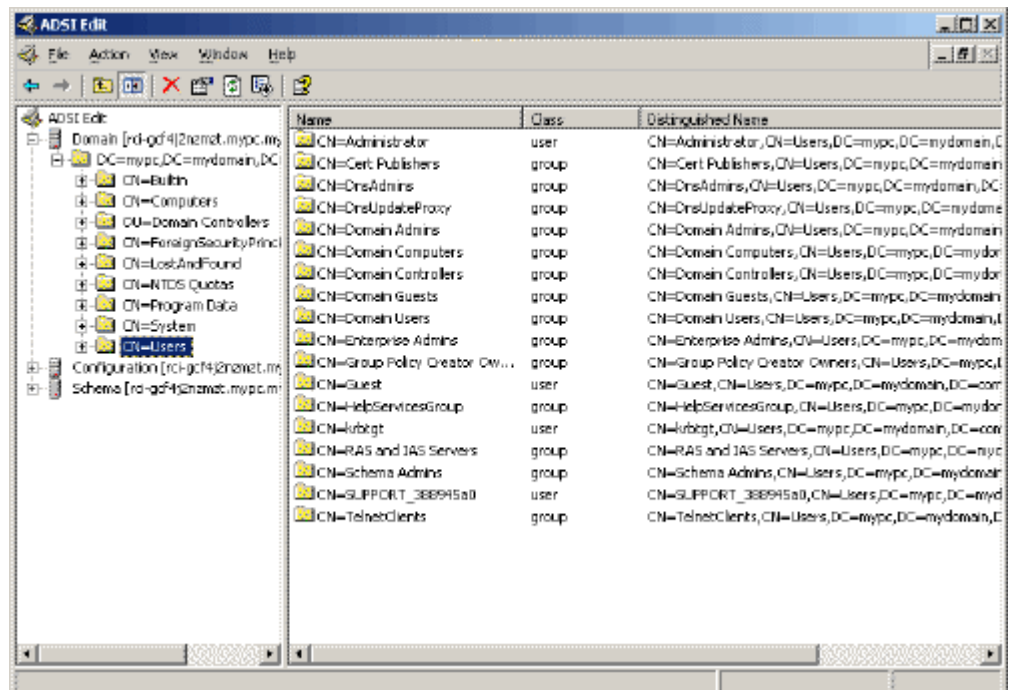
► **To edit the individual user attributes within the group rciusergroup:**

1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.

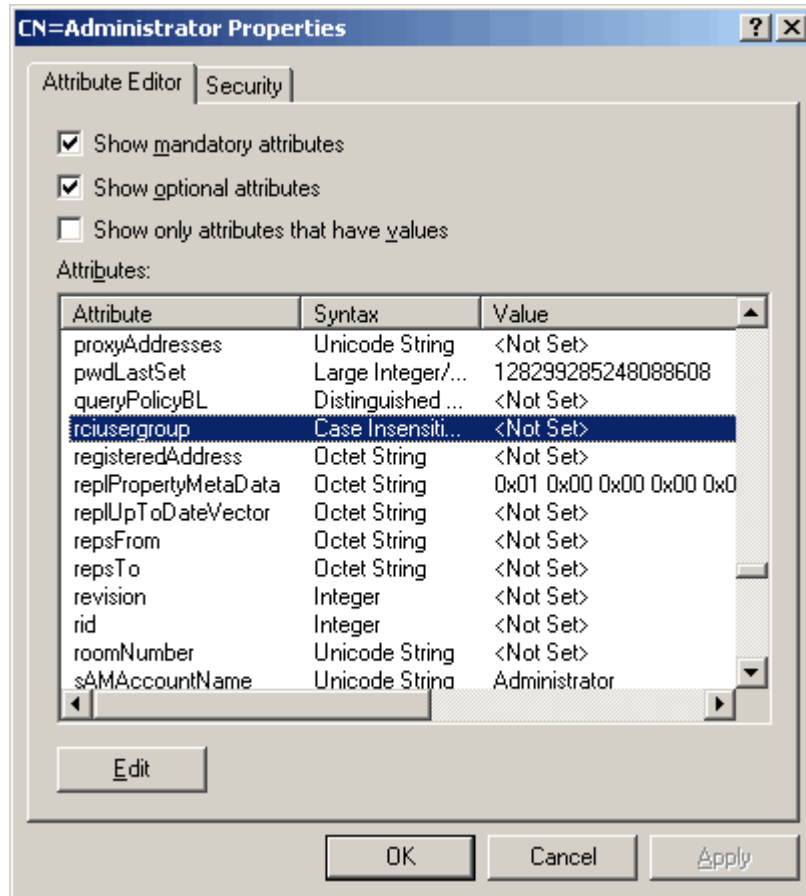
- Go to the directory where the support tools were installed. Run `adsiedit.msc`. The ADSI Edit window opens.



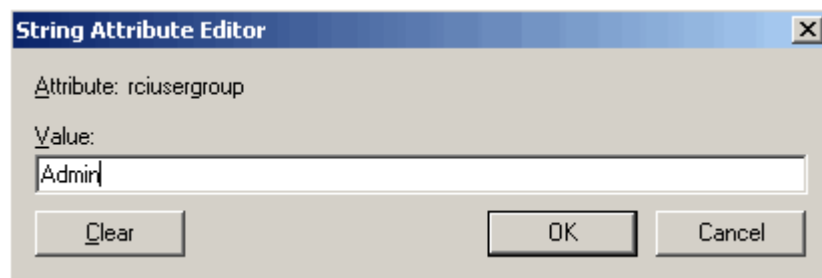
- Open the Domain.
- In the left pane of the window, select the CN=Users folder.



6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.
7. Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.



8. Click Edit. The String Attribute Editor dialog appears.
9. 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.....187
Bracket Installation189

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

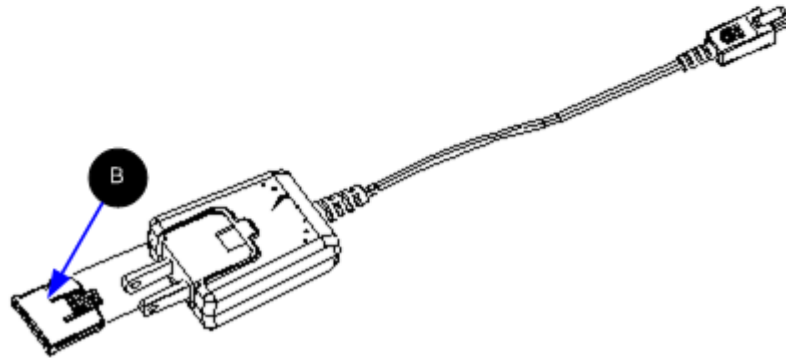
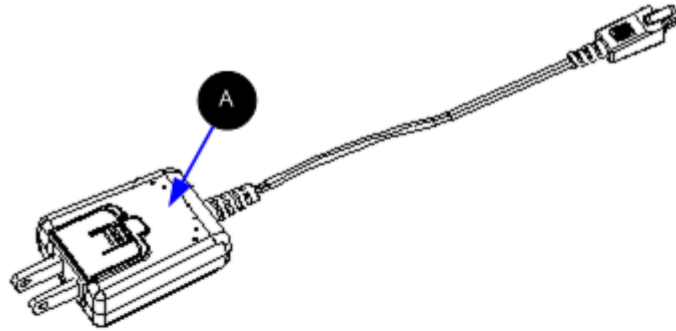




Diagram key

	AC/DC power adaptor
	Attachment cover. Push to remove.

Attach the Clip to AC-DC Power Adapter

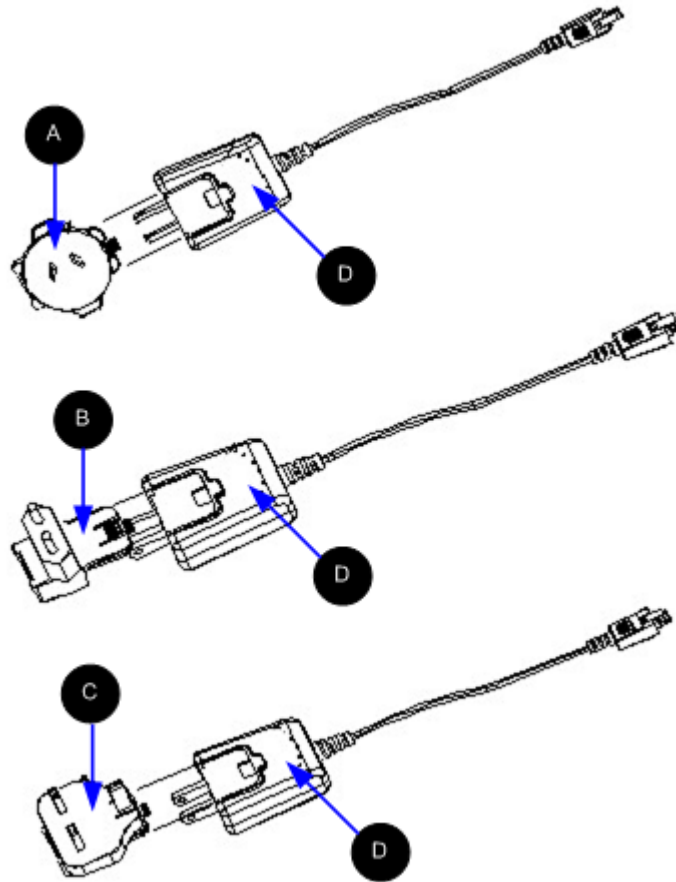


Diagram key	
A	Australian clip
B	EU clip
C	UK clip
D	Power adaptor

Bracket Installation

1. Remove the screws from the KX II-101.

- Slide the left and right panels off the KX II-101.

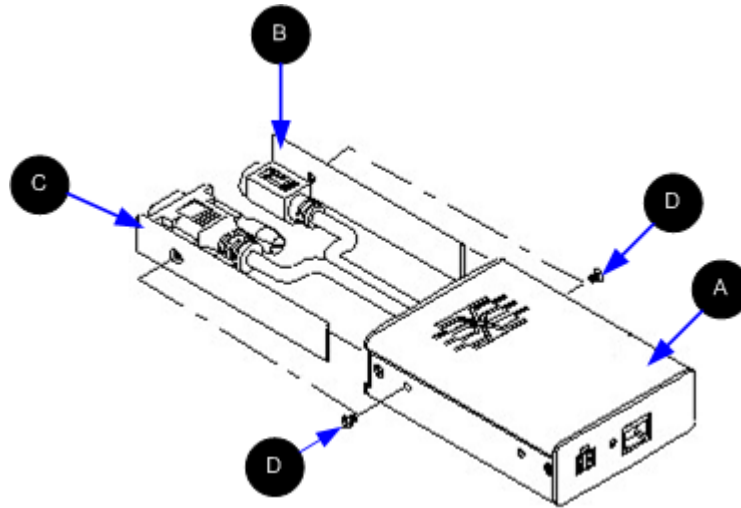
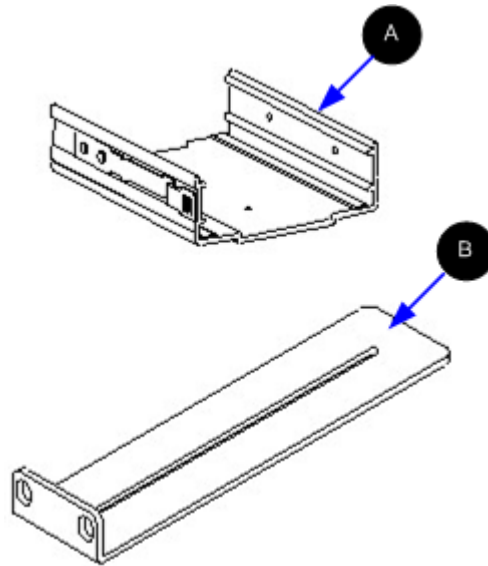




Diagram key	
A	KX II-101
B	Right panel
C	Left panel
D	Screws

KX II-101 Bracket Parts

Diagram key

	U bracket
	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.

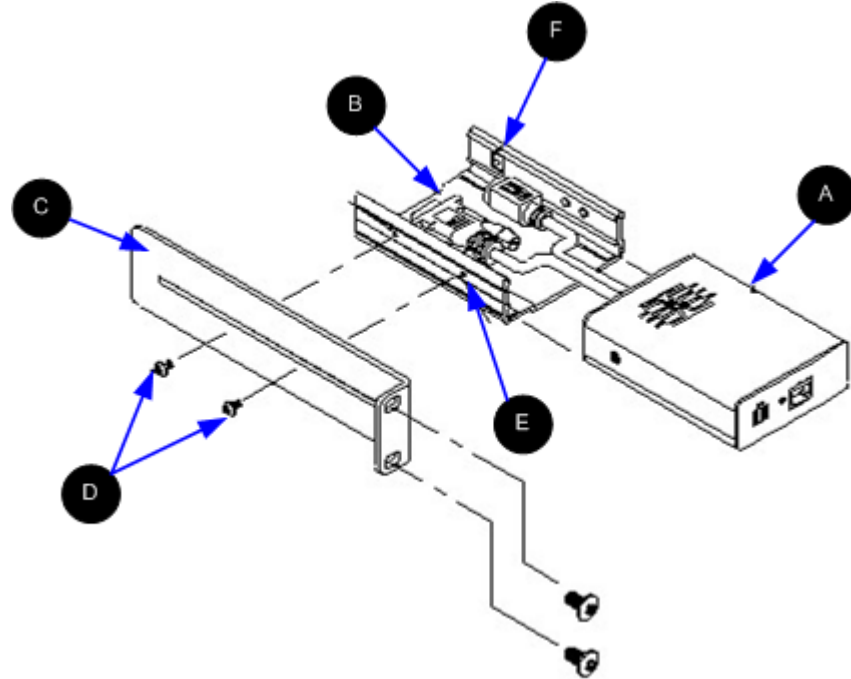


Diagram key	
A	KX II-101
B	U bracket
C	L bracket
D	Screws
E	Mounting hole
F	Latch lever

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.

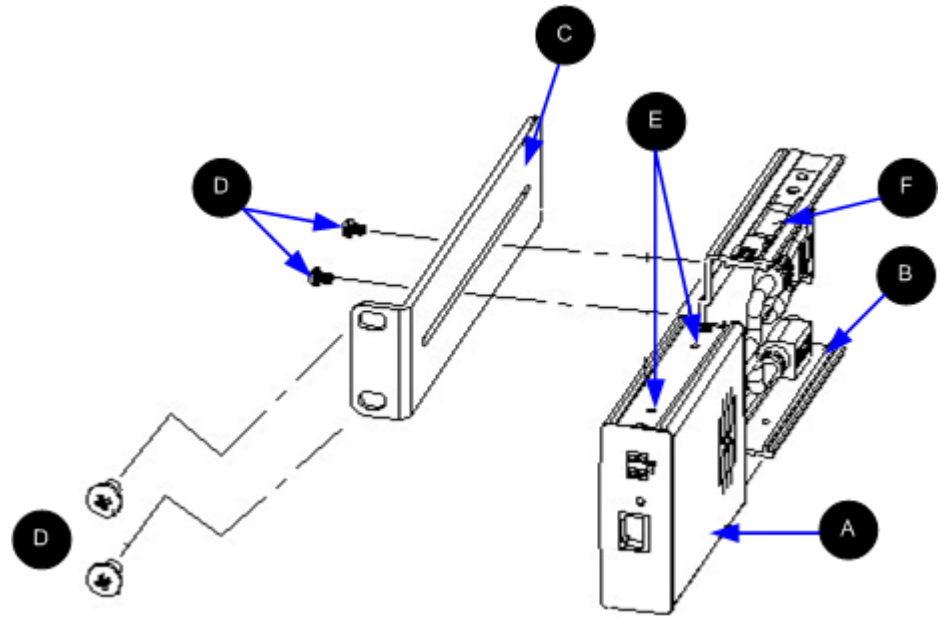


Diagram key	
A	KX II-101
B	U bracket
C	L bracket
D	Screws
E	Mounting hole
F	Latch lever

Appendix D Informational Notes

In This Chapter

Java Runtime Environment (JRE)	194
Keyboard, Video and Mouse Notes.....	194

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 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 Java Runtime Environment (JRE) version 1.5 for optimum performance, but the KX II-101 Remote Console and MPC will function with JRE version 1.6.x and higher with the exception of 1.6.2.

Note: In order for multi-language keyboards to work in the KX II-101 Remote Console (Virtual KVM Client), 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 may not function properly 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, the KX II-101 and a 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	BIOS and virtual media can be accessed for local and remote keyboards using a Newlink USB to PS/2 adapter. Set the Host Interface to PS/2 on the Keyboard/Mouse Setup page. See Keyboard/Mouse Setup (on page 103).
Dell Dimension 2400– BIOS A05	Set the Host Interface to PS/2 on the Keyboard/Mouse Setup page. See

Keyboard	Configuration to use
	Keyboard/Mouse Setup (on page 103).
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 103).
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 103).

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 103).
- Verify that the Enable Absolute Mouse and Use Full Speed checkboxes on the Port page are not selected. See **Port Configuration** (on page 115).
- 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 31).

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 • 178

A

Absolute Mouse Mode • 54
Accessing the KX II-101 Using the CLI • 158
AC-DC Adapter and Rack Mount • 6, 187
AC-DC Adapter Clip Fitting • 187
Adding a New User • 80
Adding a New User Group • 73
Adding Attributes to the Class • 182
Adding, Deleting, and Editing Favorites • 38
Adjusting Video Settings • 48
Admin Port • 1, 22, 28, 88, 94, 104
Admin Port Pinout Information • 178
Administration Features • 5
Advanced USB Connection Settings • 129
Alternate RADIUS Authentication Errors • 87, 89
Alternate RADIUS Authentication Settings • 75, 77, 78, 87, 88
Analog KVM Switch • 104, 123
Apple Macintosh® Settings • 14
Assigning an IP Address • 9, 24
Attach the Brackets to KX II-101 for Horizontal Mount • 191
Attach the Brackets to KX II-101 for Vertical Mount • 192
Attach the Clip to AC-DC Power Adapter • 189
Audit Log • 142
Authentication Settings • 81
Auto-Sense Video Settings • 51

B

Backup and Restore • 144
Basic USB Connection Settings • 127
BIOS Access Limitation from a Local Keyboard • 195
Blocking and Unblocking Users • 81
Bracket Installation • 189
Building a Keyboard Macro • 46

C

CC Unmanage • 167
CD-ROM/DVD-ROM/ISO Images • 69
Certified Modems • 107, 175
Changing a Password • 97

Checking Your Browser for AES Encryption • 136, 138
CLI Commands • 157, 162
CLI Prompts • 160
CLI Syntax -Tips and Shortcuts • 161
Command Line Interface (CLI) • 104, 157
Common Commands for All Command Line Interface Levels • 161
Compaq Alpha and IBM P Server Mouse Mode Limitation • 196
Completion of Commands • 161
Conditions when Read/Write is Not Available • 68, 69
Configuration • 164
Configure the KX II-101 Using a Terminal Emulation Program (Optional) • 9, 23, 28, 160
Configure the KX II-101 Using the Remote Console • 23
Configuring Direct Port Access • 25
Configuring Event Management - Settings • 110, 111
Connecting the Power Strip • 116, 118
Connecting to a KVM Target Server • 1, 40
Connecting to Virtual Media • 68
Connection Information • 45
Connectors • 7, 175
Controlling a Power Strip Device • 118, 121, 122
Create User Groups and Users • 28
Creating a New Attribute • 181
Ctrl+Alt+Del Macro • 52

D

Date/Time Settings • 108
Debug • 162, 163
Default Login Information • 8
Device Diagnostics • 155
Device Information • 143
Device Management • 26, 98
Device Services • 101, 158
Diagnostics • 151, 162, 163
Disconnecting a KVM Target Server • 42
Disconnecting Virtual Media • 67, 71
Discovering Raritan Devices on the KX II-101 Subnet • 37
Discovering Raritan Devices on the Local Subnet • 36

E

Editing rcusergroup Attributes for User Members • 184
Enable Direct Port Access • 31
Encryption & Share • 1, 124, 131, 135, 138
Event Management • 109
Event Management - Destinations • 111

F

Factory Reset • 148
Favorites List Page • 36, 37
File Server Setup (File Server ISO Images Only) • 66, 67
FIPS 140-2 Support Requirements • 136, 138
From LDAP • 180
From Microsoft Active Directory • 180

G

Getting Started • 9
Group-Based IP ACL (Access Control List) • 75

H

Help Options • 60
HP UX RX 1600 Keyboard and Mouse Configuration • 196

I

IBM AIX® Settings • 14
Identify the Clip Type • 187
Implementing LDAP/LDAPS Remote Authentication • 82, 85
Implementing RADIUS Remote Authentication • 1, 81, 85, 88, 94
Informational Notes • 194
Installation and Configuration • 8, 165
Intelligent Mouse Mode • 55
Interface Command • 165
Interfaces • 5, 31
Introduction • 1
IP Access Control • 139

J

Java Runtime Environment (JRE) • 194

K

Keyboard Macros • 45
Keyboard Options • 45

Keyboard, Video and Mouse Notes • 194
Keyboard/Mouse Setup • 103, 123, 195, 196
KX II-101 Bracket Parts • 191
KX II-101 Console Navigation • 32
KX II-101 Help • 1
KX II-101 Overview • 2
KX II-101 Remote Console Interface • 31, 32
KX II-101 Specifications • 170

L

LAN Interface Settings • 98, 100
Linux® Settings • 13
Listports Command • 162, 166
Local Drives • 68
Local User Port • 23
Logging On • 159
Logging Out • 40
Login Limitations • 131, 132

M

Maintenance • 142
Manage Favorites Page • 36
Managing Favorites • 35
Managing KVM Target Servers (Port Page) • 116, 118
Managing Power Associations • 120
Managing USB Connections • 126
Modem • 106
Modem Access Cable Connections • 107, 108
Modifying an Existing User • 80
Modifying an Existing User Group • 78
Modifying and Removing Keyboard Macros • 47
Mounting • 6
Mouse Modes • 11
Mouse Options • 52
Mouse Pointer Synchronization • 53
Multi-Platform Client Interface • 40

N

Name Command • 162, 164
Naming the Power Strip (Port Page for Power Strips) • 118, 119
Naming the Target Server • 26
Navigation of the CLI • 160
Network • 22, 162, 164
Network Basic Settings • 98, 99
Network Configuration • 5
Network Interface Page • 151
Network Settings • 98, 176

Network Speed Settings • 101, 177
 Network Statistics Page • 151
 Note on Microsoft Active Directory • 28
 Note to CC-SG Users • 27

O

Optional Accessories • 7
 Overview • 8, 40, 62, 127, 157, 167

P

Package Contents • 7
 Ping Host Page • 153
 Port Access Page • 33
 Port Action Menu • 33
 Port Configuration • 14, 115, 196
 Power • 6, 17
 Power Control • 116, 118
 Power Controlling a KVM Target Server • 41
 Prerequisites for Using Virtual Media • 65, 67
 Product Features • 5
 Product Photos • 4
 PS/2 Configuration • 20

R

RADIUS Communication Exchange
 Specifications • 90
 Raritan Power Strip Control • 105
 Rebooting • 149
 Refresh Screen • 51
 Related Documentation • 2
 Relationship Between Users and Groups • 73
 Remote Authentication • 27
 Remove the Attachment Cover from AC-DC
 Power Adapter • 188
 Removing a KX II-101 from CC-SG
 Management • 168
 Renaming a Port • 117
 Resetting the KX II-101 Using the Reset
 Button • 124, 137
 Returning User Group Information • 180
 Returning User Group Information from Active
 Directory Server • 84
 Returning User Group Information via RADIUS
 • 90
 Running a Keyboard Macro • 47

S

Security Management • 131
 Security Settings • 131
 Serial Port Settings • 104
 Setlog Command • 162, 163

Setting a New Password • 23
 Setting Permissions • 77, 78
 Setting Permissions for an Individual Group •
 78, 80
 Setting Port Permissions • 74
 Setting the Registry to Permit Write
 Operations to the Schema • 181
 Setting the Server Video Resolution • 9, 10
 Single Mouse Cursor • 56
 Specifications • 170
 SSH Access from a UNIX/Linux Workstation •
 159
 SSH Access from a Windows PC (Shared
 KSX II, KX II 101, SX) • 158
 SSH Access when Alternate RADIUS
 Authentication is Enabled • 1, 88, 94, 159
 SSH Connection to the KX II-101 • 158
 Standard Mouse Mode • 54
 Step 1
 Configure the Target Server • 8, 9
 Step 2
 Configure Network Firewall Settings • 8, 15
 Step 3
 Connect the KX II-101 • 8, 16
 Step 4
 Configure the KX II-101 • 8, 23
 Strong Passwords • 97, 131, 133
 Sun Blade™ Video, Keyboard, and Mouse
 Support Limitation • 194
 Sun Keyboard Key Support Limitations • 195
 Sun® Solaris™ Settings • 13
 Sun™ Video Resolution • 10
 Supported Browsers • 175
 Supported Keyboard Languages • 172
 Supported Operating Systems (Clients) • 173
 Supported Protocols • 27
 Supported Video Resolutions • 171
 System Management Features • 5

T

Target Server • 18
 TCP and UDP Ports Used • 175
 Terminology • 6
 Tool Options • 57
 Trace Route to Host Page • 154

U

Updating the LDAP Schema • 84, 180
 Updating the Schema Cache • 184
 Upgrade History • 148
 Upgrading Firmware • 146

Index

- USB Configuration • 18
- User Authentication Process • 1, 92, 159
- User Blocking • 81, 131, 134
- User Features • 6
- User Group List • 73
- User Groups • 72
- User List • 79
- User Management • 28, 72
- Userlist Command • 162, 166
- Users • 79
- Using CC-SG in Proxy Mode • 169
- Using Virtual Media • 67

V

- Video Properties • 48
- Video Resolution • 6
- View Options • 59
- Virtual KVM Client • 33, 40
- Virtual Media • 56, 61
- VKC Connection Properties • 43
- VKC Toolbar for the KX II-101 • 41, 43, 50, 51, 52, 53, 56
- VKC Virtual Media • 56

W

- What's New in the Help • 1
- Windows 2000 and 2003 Server Keyboard Limitations • 197
- Windows 2000® Settings • 11
- Windows Vista® Settings • 12
- Windows XP®/Windows 2003® Settings • 12
- Working with Target Servers • 31, 196

▶ **U.S./Canada/Latin America**

Monday - Friday
8 a.m. - 6 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

▶ **China**

Beijing

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

▶ **India**

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

▶ **Japan**

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5991
Email: support.japan@raritan.com

▶ **Europe**

Europe

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom

Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany

Monday - Friday
8:30 a.m. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

▶ **Melbourne, Australia**

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

▶ **Taiwan**

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com