



Dominion KX II-101

User Guide Release 2.0

Copyright © 2008 Raritan, Inc.

February 2008
255-62-4031-00

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

© Copyright 2008 Raritan, Inc., CommandCenter®, Dominion®, Paragon® and the Raritan company logo are trademarks or registered trademarks of Raritan, Inc. All rights reserved. Java® is a registered trademark of Sun Microsystems, Inc. Internet Explorer® is a registered trademark of Microsoft Corporation. Netscape® and Netscape Navigator® are registered trademarks of Netscape Communication Corporation. All other trademarks or registered trademarks are the property of their respective holders.

FCC Information

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

VCCI Information (Japan)

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

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



Contents

Chapter 1	Introduction	1
	Dominion KX II-101 Overview	2
	Product Photos.....	3
	Product Features.....	4
	Interfaces	4
	Network Configuration.....	4
	System Management Features.....	4
	Administration Features	4
	User Features	5
	Power	5
	Video Resolution	5
	Mounting.....	5
	Package Contents	6
	Terminology	6
	Optional Accessories.....	6
Chapter 2	Important Information	7
	Login	7
	Default IP Address	7
	Service Pack.....	7
Chapter 3	Installation and Configuration	8
	Configuring the Target Server	8
	Setting Server Video Resolution.....	9
	Mouse Modes.....	11
	Connecting the KX II-101.....	15
	Connecting to the Target Server.....	16
	Connecting to the Network.....	20
	Powering the KX II-101	20
	Using the Admin Port.....	20
	Using the Local User Port	21
	Configuring Network Firewall Settings	21
	Configuring the KX II-101	21
	Using the Remote Console	22
	Using a Terminal Emulation Program	27

Chapter 4 Connecting to the KX II-101 32

Language Support.....	32
Java Runtime Environment (JRE).....	32
Launching the KX II-101.....	33
Enabling Direct Port Access.....	34
KX II-101 Console Layout.....	35
KX II-101 Console Navigation.....	36
KX II-101 Remote Console Menu Map.....	37
Logging Out.....	37
Managing Favorites.....	38
Manage Favorites Menu.....	39
Favorites List.....	40
Discover Devices - Local Subnet.....	42
Discover Devices - KX II-101 Subnet.....	44
Add New Favorite.....	45
Port Access Page.....	46

Chapter 5 Users, Groups, and Access Permissions 47

Users.....	47
Groups.....	47
Relationship between Users and Groups.....	48
User Management.....	49
User Management Menu.....	49
Remote Authentication.....	61
Note to CC-SG Users.....	61
Supported Protocols.....	61
Note on Microsoft Active Directory.....	61
Authentication vs. Authorization.....	61
Authentication Settings.....	62
Updating the LDAP Schema.....	69

Chapter 6 Virtual KVM Client 79

Overview.....	80
Options.....	81
Menu Tree.....	81
Toolbar.....	82
Mouse Pointer Synchronization.....	83
Mouse Synchronization Tips.....	83
Connection Menu.....	85
Properties Dialog.....	85
Connection Info.....	87
Exit.....	87

Keyboard Menu	88
Send Ctrl+Alt+Delete	88
Keyboard Macros	88
Creating a Keyboard Macro	89
Running a Keyboard Macro	91
Modifying a Keyboard Macro	91
Removing a Keyboard Macro	91
Video Menu	92
Refresh Screen	92
Auto-sense Video Settings	92
Calibrate Color	93
Video Settings	93
Mouse Menu	96
Synchronize Mouse	96
Single Mouse Cursor	97
Standard	97
Intelligent	98
Absolute	98
Virtual Media	98
Tools Menu	99
Options	99
View Menu	100
View Toolbar	100
Scaling	100
Target Screen Resolution	101
Help Menu	101
About Raritan Virtual KVM Client	101

Chapter 7 Virtual Media 102

Overview	103
Prerequisites for Using Virtual Media	105
Using Virtual Media	106
Opening a KVM Session	107
Connecting to Virtual Media	108
Local Drives	108
Conditions when Read-Write is not Available	109
CD-ROM/DVD-ROM/ISO Images	110

Contents

Disconnecting Virtual Media	111
File Server Setup (File Server ISO Images Only).....	112

Chapter 8 Device Management 114

Device Settings Menu	114
Network Settings	115
Network Basic Settings.....	116
LAN Interface Settings	118
Device Services	120
Keyboard/Mouse Settings	122
Serial Port Settings.....	123
Date/Time Settings	124
Event Management	125
SNMP Configuration	126
Syslog Configuration	127
Event Management - Destinations.....	128
SNMP Agent Configuration	129
SNMP Trap Configuration.....	129
Port Configuration	131

Chapter 9 Power Control 133

Overview	133
Connect the Power Strip.....	133
Name the Power Strip (Port Page for Power Strips).....	135
Associate KVM Target Servers to Outlets (Port Page)	136
Displaying the Outlet Associations.....	140
Control the Powerstrip Device	141

Chapter 10 Security Settings 143

Security Settings Menu	143
Security Settings	144
Login Limitations	145
Strong Passwords.....	146
User Blocking.....	147
Encryption and Share	148
Checking Your Browser for AES Encryption	151

IP Access Control.....	151
Chapter 11 Maintenance	154
Maintenance Menu.....	154
Audit Log.....	155
Device Information.....	156
Backup and Restore.....	157
Firmware Upgrade.....	159
Upgrade History.....	161
Reboot	161
Chapter 12 Command Line Interface (CLI)	163
Overview	163
Accessing the KX II-101 Using the CLI.....	164
SSH Connection to the KX II-101.....	164
SSH Access from a Windows PC	164
SSH Access from a UNIX Workstation	165
Login	165
Navigation of the CLI	166
CLI Prompts.....	166
Completion of Commands.....	166
CLI Syntax -Tips and Shortcuts.....	167
Common Commands for All Command Line Interface Levels	167
CLI Commands.....	168
Diagnostics.....	169
Configuration.....	170
Listports Command	172
Userlist Command	172

Contents

Chapter 13	Diagnostics	173
<hr/>		
	Diagnostics Menu	173
	Network Interface Page	174
	Network Statistics Page	174
	Ping Host Page	177
	Trace Route to Host Page	178
	Device Diagnostics	179
Chapter 14	CC Unmanage	181
<hr/>		
	Overview	181
	Removing KX II-101 from CC-SG Management	182
	Using CC-SG in Proxy Mode	183
Appendix A	Specifications	184
<hr/>		
	KX II-101	184
	Connectors	185
	Raritan Remote Client Software	185
Appendix B	Rack Mount	186
<hr/>		
	AC-DC Adapter Clip Fitting	186
	Identify Clip Type	186
	Remove Attachment Cover from AC-DC Power Adapter	187
	Attach Clip to AC-DC Power Adapter	187
	Bracket Installation	188
	KX II-101 Bracket Parts	189
	Attach Brackets to KX II-101 for Horizontal Mount	190
	Attach Brackets to KX II-101 for Vertical Mount	190
Index		193
<hr/>		

Chapter 1 Introduction

In This Chapter

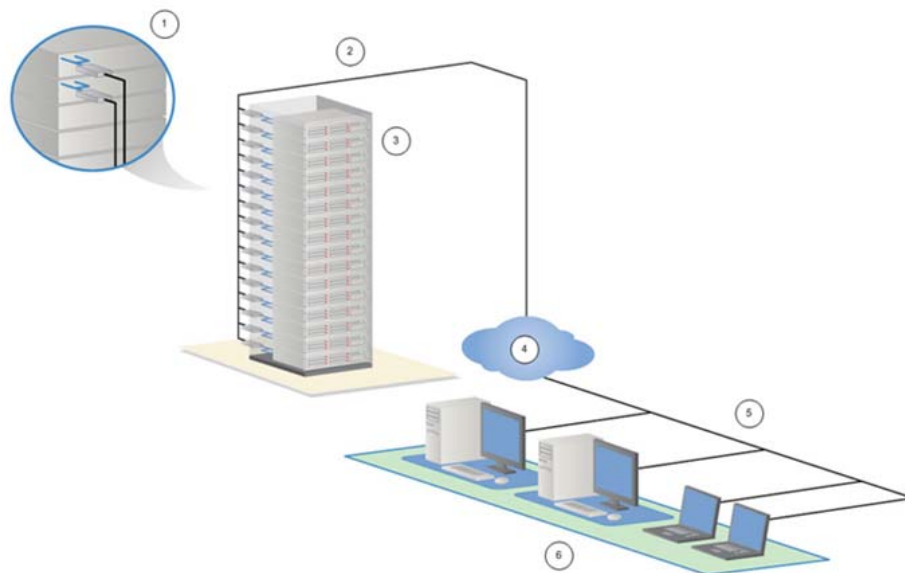
Dominion KX II-101 Overview	2
Product Photos.....	3
Product Features.....	4
Package Contents.....	6
Terminology	6

Dominion KX II-101 Overview

Thank you for purchasing Dominion 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 unit, 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 unit has its own IP Address. Each unit is powered via Power-over-Ethernet (PoE) or external AC-DC power pack.

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



- 1 KX II-101
- 2 LAN
- 3 Windows, Linux, and Sun servers.
- 4 TCP/IP
- 5 LAN

6 Remote (Network) Access

Product Photos



KX II-101 Units

Product Features

Interfaces

- Integrated PS/2 KVM connection
- Optional USB connection for control and Virtual Media
- Serial Admin port for initial device setting and diagnostics and external modem access
- Ethernet LAN port supporting 10/100-base-T auto-sensing, 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 upgradeable over Ethernet
- Failsafe firmware upgrade capability
- Admin settable clock or synchronization with Network Time Protocol (NTP/SNTP)
- Local time-stamped administrator activity log SNMP V2 agent that can be disabled by the administrator
- Supports RADIUS and LDAP 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 appliance

User Features

- Web-based access through common browsers
- Intuitive Graphical User Interface (GUI)
- “PC Share” mode enabling 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 provision
- Alternative power by an external AC-DC power pack

Video Resolution

- Up to 1600X1200 at up to 60 Hz resolution

Mounting

- Rack mounting bracket
- See ***Rack Mount*** (on page 186) for information.

Package Contents

Each KX II-101 unit ships with:

- Main Unit KX II-101 - KVM over IP Dongle
- USB Type A to Type B-mini connector
- Power Adaptor Kit - AC-DC 6VDC
- Three additional power outlet plugs for worldwide use
- Mini-DIN to DB9 serial cable
- Mounting bracket kit
- Raritan User Manuals & Quick Setup Guides CD-ROM
- Printed Quick Setup Guide
- Printed Application Notes (if applicable)
- Printed Technical Notes (if applicable)

Terminology

Target Server	Server to be accessed remotely via KX II-101 and its connected KVM configuration.
Remote PC	A Windows, Linux, Solaris, or Apple Macintosh® computer used to access and control target servers connected to the KX II-101.
Admin serial port	The KX II-101 is provisioned with an Admin serial port. Connect the serial port on the PC to the Admin serial port of the KX II-101 unit using the included Mini-DIN to DB9 cable. Then use a standard emulation software package (e.g., HyperTerminal) to access the Admin serial port. The admin serial port is used for network configuration.
Local User port	A port to enable a user in immediate proximity to the target server to use the native keyboard and mouse without unplugging the KX II-101.
Virtual Media	Enables a KVM target server to remotely access media from client PC and network file servers.

Optional Accessories

- DB15 to PS/2 and VGA Local User Cable

See *Connectors* (on page 185) for information.

Chapter 2 Important Information

In This Chapter

Login.....	7
Default IP Address	7
Service Pack	7

Login

- The default KX II-101 login user name is **admin** and the password is **raritan**. This user has administrative privileges.
- Passwords are case sensitive and must be entered in the exact case combination in which they were created.
- The default password raritan must be entered entirely in lowercase letters.
- To ensure security, change the default password as soon as possible.

Default IP Address

KX II-101 ships with a static default IP address of 192.168.0.192. On a network without a DHCP server, you must configure a new static IP address, net mask, and gateway addresses using either the KX II-101 serial admin console or the KX II-101 Remote Console.

See *Assigning an IP Address* (on page 23) for information about assigning an IP address to the KX II-101 using the Remote Console. See *Using the Local Serial Console* (see "Using a Terminal Emulation Program" on page 27) for information about setting an IP address using the Serial Admin Console.

Service Pack

- KX II-101 users with Microsoft Internet Explorer version 5.01 or Windows 2000 must upgrade to Service Pack 4 (SP4) or higher.

Chapter 3 Installation and Configuration

In This Chapter

Configuring the Target Server	8
Connecting the KX II-101	15
Configuring Network Firewall Settings	21
Configuring the KX II-101	21

Configuring the Target Server

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

1. *Configuring Target Server* (see "Configuring the Target Server" on page 8).
2. *Configuring Network Firewall Settings* (on page 21).
3. *Connecting the KX II-101* (on page 15).
4. *Configuring the KX II-101* (on page 21).

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

Setting 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 KX II-101, and that the signal is non-interlaced. KX II-101 supports the following video resolutions:

Text Modes

640x480 @ 60Hz	1024x768 @ 60Hz
640x480 @ 72Hz	1024x768 @ 70Hz
640x480 @ 75Hz	1024x768 @ 75Hz
640x480 @ 85Hz	1024x768 @ 85Hz
800x600 @ 56Hz	1152x864 @ 60Hz
800x600 @ 60Hz	1152x864 @ 75Hz
800x600 @ 72Hz	1280x1024 @ 60Hz
800x600 @ 75Hz	1600x1200 @ 60Hz
800x600 @ 85Hz	

Setting 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 Server Video Resolution* (on page 9).

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

Command Line Resolution

➤ *To check the command line resolution:*

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

Configuring the Target Server

➤ *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 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 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 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 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 the following paragraphs in this section.

This section describes the mouse configurations necessary for different systems.

Windows Vista

➤ *To configure the mouse:*

1. Choose Start > Settings > Control Panel > Mouse.
2. Click the Pointer Options tab. In the Motion group:
 - a. Set the mouse motion speed setting exactly to the middle speed.
 - b. Deselect the Enhanced pointer precision option.
3. Click OK.

➤ *To disable animation and fade effects:*

1. From the Windows Start menu, choose Control Panel > System > Advanced system settings. The System Properties dialog opens.
2. Click the Advanced tab.
3. Select the Settings button in the Performance group. The Performance Options dialog opens.
4. Under Custom options, deselect the following checkboxes:
 - Animate controls and elements inside windows
 - Animate windows when minimizing and maximizing

Configuring the Target Server

- Fade or slide menus into view
 - Fade or slide ToolTips into view
 - Fade out menu items after clicking
5. Click OK.
 6. Close the Control Panel.

Windows XP Settings

On a KVM target server running Microsoft Windows XP, disable the “Enhanced Pointer Precision” option, and set the mouse motion speed exactly to the middle speed setting. These parameters are found in Control Panel ® Mouse ® Mouse Pointers.

Note: For a target server running Windows 2000 or XP, you may wish to create a username to be used only for remote connections through 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.

Note: Windows XP and 2000 login screens revert to pre-set 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 2000 Settings

On a target server running Microsoft Windows 2000, set the mouse pointer acceleration to “none” and the mouse motion speed exactly to the middle speed setting. These parameters are found in Control Panel® Mouse.

Linux Settings

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

As mentioned above, please ensure that a target server running Linux is using a resolution supported by 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 KX II-101.
4. Check blanking times (+/- 40% of VESA standard).
5. Restart 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:

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

A target server running the Solaris operating system must output VGA video (H-and-V sync, not composite sync). To change your Sun video card output from composite sync to the non-default VGA output, first issue the Stop+A command to drop to bootprom mode. Then, issue the command:

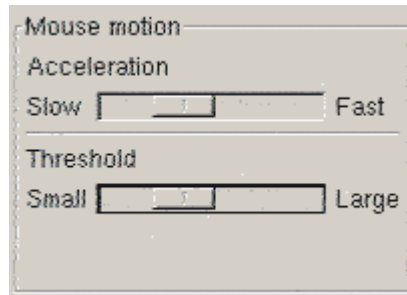
```
#eeprom output-device=screen:r1024x768x75
```

Configuring the Target Server

to change the output resolution. 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 KX II-101. HD15 Suns with separate sync output require an APKMSUN Raritan guardian for use with KX II-101. KX101 supports only the PS/2 version with the use of an APSUSB adaptor (composite sync is not supported).

On a target server running the Solaris operating system, set the mouse acceleration value to exactly 1 and threshold to exactly 1. Set this at the graphical user interface (shown below), or with the command line “xset mouse a t” where “a” is the acceleration and “t” is the threshold.



Apple® Macintosh Settings

Use the Absolute Mouse Synchronization.

Connecting the KX II-101

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



- 1 Attached Monitor and PS/2 Cable (See item 3.).

Connecting the KX II-101

- 2 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 in order to utilize the Absolute Mouse Sync or Virtual Media features.
- 3 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.
- 4 LOCAL USER port. Use to connect a local keyboard, video, and mouse directly to the target server using an optional PS/2 cable.
- 5 Ethernet LAN/PoE Port. Provides LAN connectivity and power if using a PoE LAN connection.
- 6 Power Connector. Connects the power supply if you are not using a PoE (power over Ethernet) LAN connection.
- 7 Backlit LED power ON and boot-up indicator. Provides feedback on the operating status of the device.
- 8 Admin Port. Use to do one of the following:
 - 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.

Connecting to the Target Server

The KX II-101 can use either the integrated PS/2 cables or the included USB cable to connect to the target server. Before connecting, configure your target server's video to a supported resolution and refresh rate as described in *Setting Server Video Resolution* (on page 9).

PS/2 Configuration

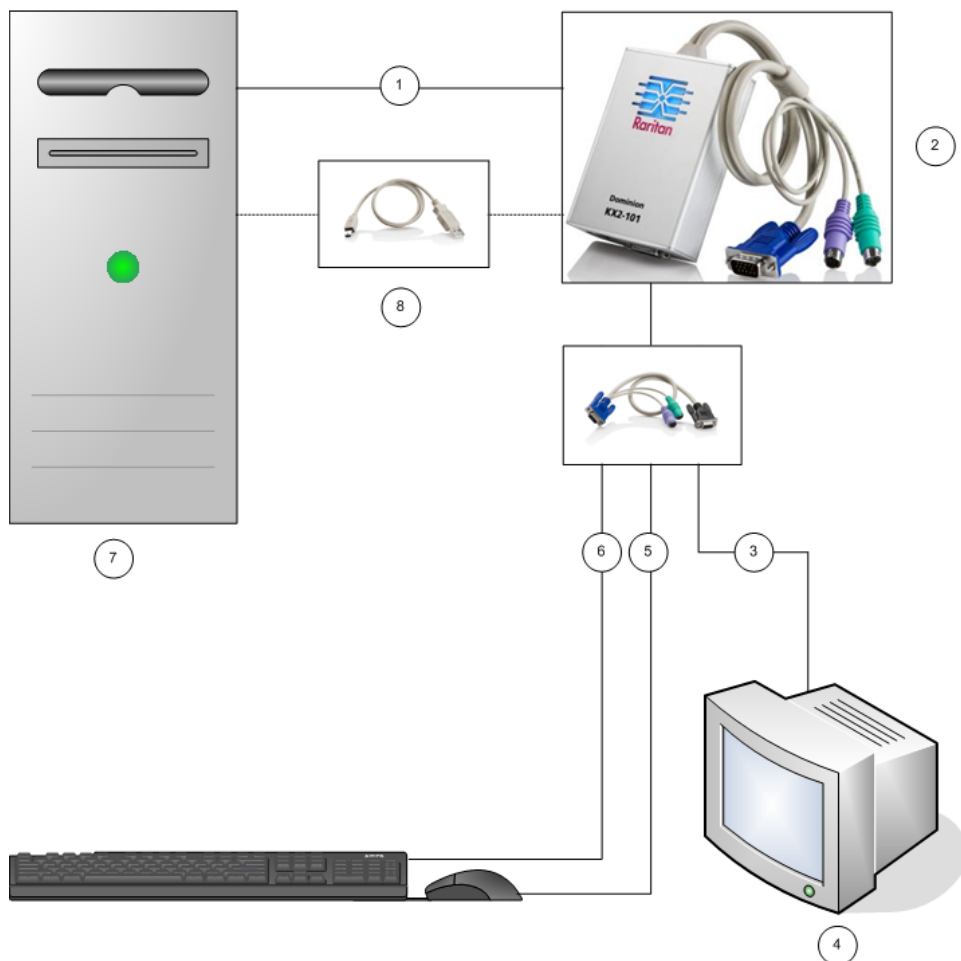
- *To configure the KX II-101 for use with a PS/2 target server:*
1. Use the attached PS/2 keyboard, video, and mouse cabling to connect the KX II-101 to the target server.
 2. Use the optional PS/2 cabling to attach the local keyboard, video, and mouse to the Local User port of the KX II-101.

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

3. 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.

When you finish, you should have connections like those shown in the illustration below:

PS/2 Configuration



- 1 Integrated PS/2 keyboard, video, and mouse connections from KX II-101 to target server.
- 2 KX II-101.
- 3 Video connection to local monitor (optional cable).
- 4 Local monitor.

Connecting the KX II-101

- 5 PS/2 connection from KX II-101 to mouse (optional cable).
- 6 PS/2 connection from KX II-101 to keyboard (optional cable).
- 7 Target server.
- 8 Included mini-USB to USB connector from KX II-101 to target server for Virtual Media connectivity.

USB Configuration

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

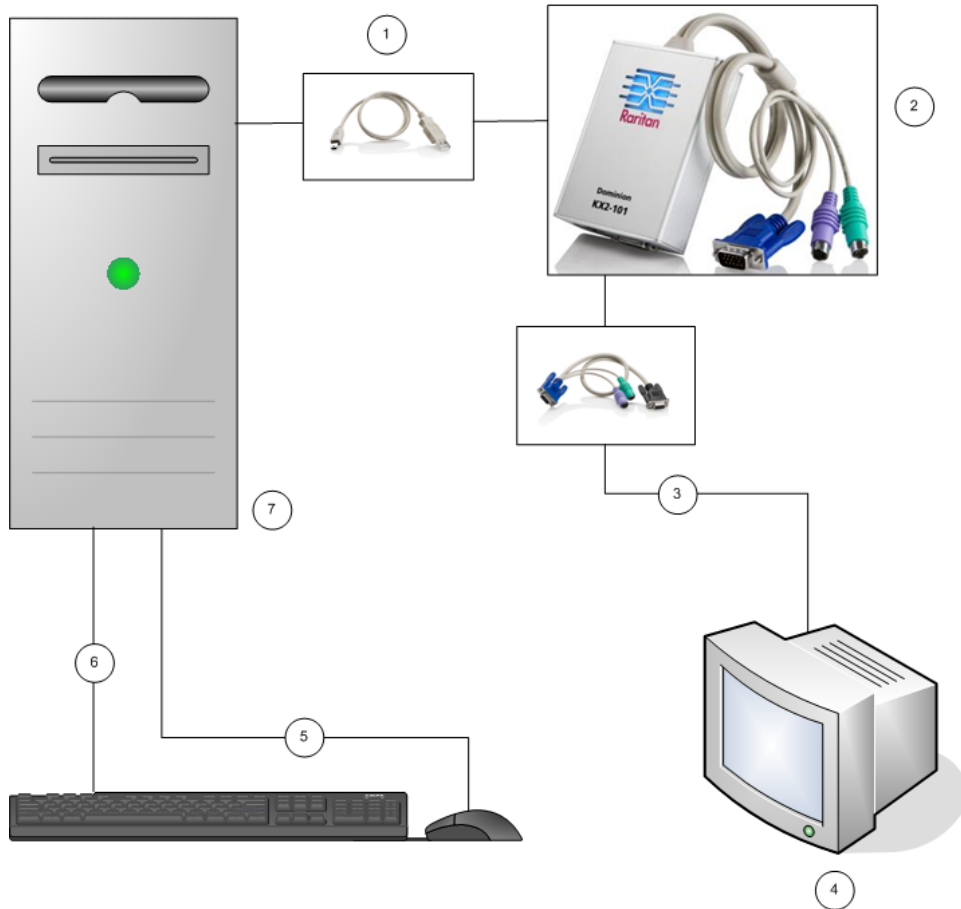
1. Connect the mini-USB connector to the KX II-101 and the USB connector to a USB port on the target server.
2. Use the included PS/2 DKX2-101-LPKVMC cabling to attach only the local video to the Local User port of the KX II-101.

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

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

When you finish, you should have connections like those show in the following illustration:

USB Configuration



- 1 Included mini-USB to USB cable from KX II-101 to target server.
- 2 KX II-101.
- 3 Video connection to local monitor (optional cable).
- 4 Local monitor.
- 5 USB connection from target server to mouse.
- 6 USB connection from target server to keyboard.
- 7 Target server.

Connecting to the 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 10Mbps. The green light indicates a 100Mbps connection speed.

Powering the KX II-101

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 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.

Using the 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: to 115,200 Baud, 8 data bits, 1 stop bit, no parity, and no flow control.

For information about configuring the KX II-101 using the ADMIN port, see Using a Terminal Emulation Program.

Using the Local User Port

The KX II-101 is available with optional video and PS/2 cables 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.

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

Configuring 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.

In order to take advantage of KX II-101's web-access capabilities, the firewall must allow inbound communication on TCP Port 443 - the standard TCP port for HTTPS communication. In order to take advantage of 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.

Configuring 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 unit to have a network connection to your workstation.
- Using a terminal emulation program like HyperTerminal, which requires a direct connection from the unit'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.

Using the Remote Console

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

To configure the KX II-101, you:

- Set a new password to replace the default
- Assign an IP address
- Name the target server
- Create users and groups

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 on to a workstation with network connectivity to your KX II-101 unit.
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 unit:

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; retype the new password in 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 Settings. The Network Basic Settings page opens.

Home > Device Settings > Network Settings

Network Basic Settings

Device Name *

DominionKX2-101

IP auto configuration

DHCP

Preferred host name (DHCP only)

IP address

192.168.50.241

Subnet mask

255.255.255.0

Gateway IP address

192.168.50.126

Primary DNS server IP address

192.168.50.114

Secondary DNS server IP address

192.168.50.112

OK Reset To Defaults Cancel

2. In the Device Name field, specify a meaningful name for your KX II-101 unit; up to 16 alphanumeric and special characters, 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 Dominion 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.

Configuring Direct Port Access

➤ *To configure direct port access:*

1. Choose Device Settings > Device Services. The Device Services page appears.
2. Select the Enable Direct Port Access via URL checkbox.

Configuring the KX II-101

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.

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

5. Click OK to save this information.

Naming the Target Server

1. Attach the KX II-101 to the target server (if you have not already done so), as described in *Connecting to the KX II-101* (on page 32).
2. Choose Device Settings > Port Configuration. The Port Configuration page opens.

3. Click Port Name for the target server. The Port Page opens.

4. Type a name (up to 32 alphanumeric and special characters).
5. Click OK.

Creating Users and Groups

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

➤ *To create a user group:*

1. Open the Group page using one of these methods:
 - a. Choose User Management > Add New User Group, or
 - b. Click the Add button from the User Group List page.
2. Type a descriptive name for the new user group into the Groupname field.
3. Set the Permissions for the group. Check the checkboxes before the permissions you want to assign to all users belonging to this group.
4. Set the Port Permissions (Access, VM Access, and Power Control). Specify the server ports that can be accessed by users belonging to this group and the type of access. Please note that the default for VM (virtual media) Access, like all port permissions is off. To use virtual media, the permission must be enabled.

5. Click OK.

➤ *To create a new user:*

1. Open the User page using one of these methods:
 - a. Choose User Management > Add New User, or
 - b. Click the Add button from 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; retype the password in the Confirm Password field (up to 64 characters).
5. Select 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 (Admin, <Unknown>, Individual Group). If you do not want to associate this user with an existing User Group, select Individual Group from the drop-down list.
6. Click OK.

Using a Terminal Emulation Program

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 using the *Using the Admin Port* (on page 20) for information.

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:*

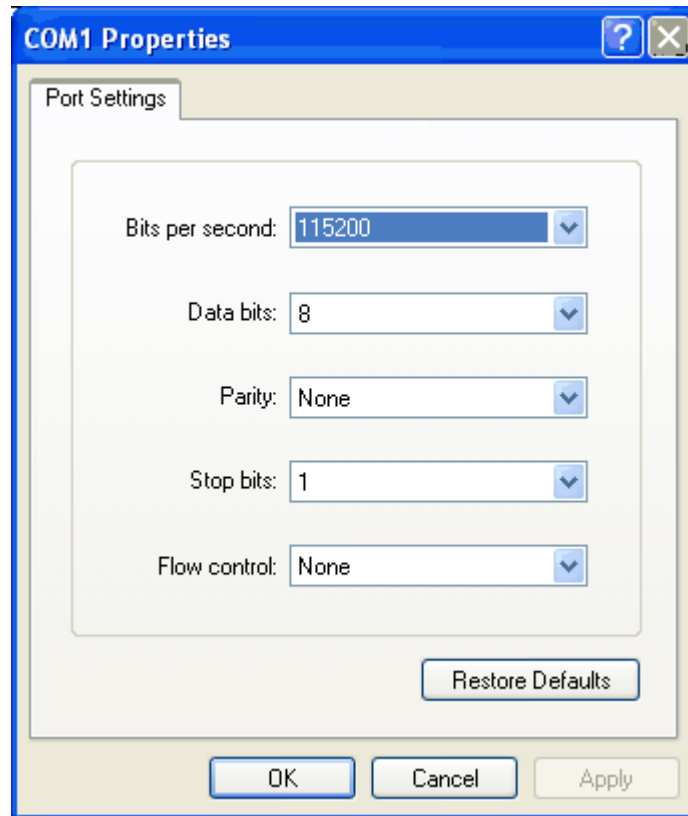
1. Connect the KX II-101 to a local PC using the included RS-232 serial cable.

Connect to the Admin port on the KX II-101 and the COM1 port on the PC.

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

Configuring the KX II-101

- Flow control: None



4. Connect to the KX II-101.

The login screen appears.



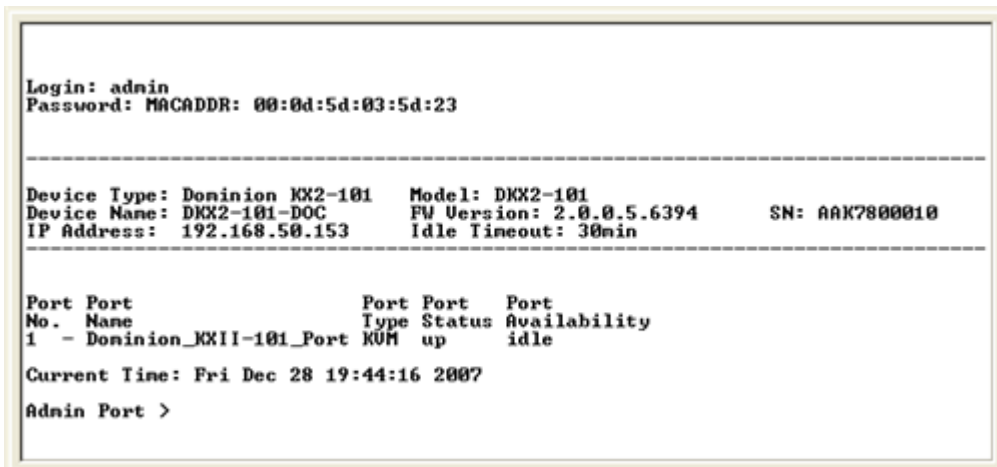
5. Type the administrator user name and press Enter.

You are prompted to enter your password.



6. Type your password and press Enter.

The Admin Port prompt appears.



7. At the Admin Port > prompt, type config and press Enter.
8. At the Config > prompt, type network and press Enter.
9. To view the current interface settings, at the Interface > prompt, type interface and press Enter.

Configuring the KX II-101

The current interface settings appear:

```

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          KVM  up       idle

Current Time: Fri Dec 28 19:52:26 2007

Admin Port > config
Admin Port > Config > network
Admin Port > Config > Network > interface

IP auto configuration: dhcp
IP address: 192.168.50.153
Netmask: 255.255.255.0
Gateway: 192.168.50.126
Ethernet mode: Autodetect

Admin Port > Config > Network > _

```

- 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 <code>ip</code> 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 <code>ipauto</code> command and the <code>none</code> option. See <code>ipauto</code> for information. After you have manually assigned an IP address once, you can use the <code>ip</code> 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> <p>auto - Automatically sets speed and interface mode based on the network.</p> <p>10hdx - 10 Mbs, half duplex.</p> <p>10fdx - 10 Mbs, full duplex</p> <p>100hdx - 100 Mbs, half duplex</p> <p>100fdx - 100 Mbs, full duplex</p>

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.
```

11. 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 4 Connecting to the KX II-101

In This Chapter

Language Support	32
Java Runtime Environment (JRE)	32
Launching the KX II-101	33
Managing Favorites	38
Port Access Page	46

Language Support

The KX II-101 provides keyboard support for the following languages: US English, Traditional Chinese, Simplified Chinese, Japanese, Korean, French, and German.

Note: You can use the keyboard for Chinese, Japanese, and Korean for display only; local language input is not supported at this time for KX II-101 Remote Console functions.

Language Configuration on Linux

Refer to **Keyboard Type (MPC only)** in the *MPC-RRC User Guide* for information about configuring foreign language keyboards on Linux.

Java Runtime Environment (JRE)

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

The KX II-101 Remote Console and MPC require the JRE to function. The KX II-101 Remote Console checks the Java version; if the version is incorrect or outdated, you will be prompted to download a compatible version.

Raritan recommends using Java Runtime Environment (JRE) version 1.5 for optimum performance, but the KX II-101 Remote Console and MPC will function with JRE version 1.4.2_05 or greater (with the exception of JRE 1.5.0_02), including JRE 1.6.x except for 1.6.2.

Note: In order for multi-language keyboards to work in the KX II-101 Remote Console (Virtual KVM Client) please install the multi-language version of Java Runtime Environment (JRE).

Launching the KX II-101

Important: Regardless of the browser used, you must allow pop-ups from the Dominion device's IP address to launch the KX II-101 Remote Console.

Depending on your browser and security settings, you may see various security and certificate warnings. It is necessary to accept these warnings to launch the KX II-101 Remote Console.

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

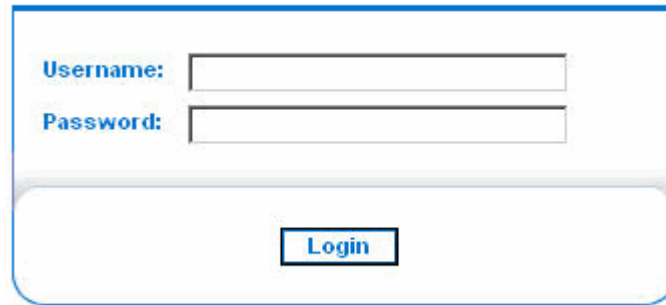
- In the future, do not show this warning
- Always trust content from this publisher

➤ *To launch the KX II-101 Remote Console:*

1. Log on to any workstation with network connectivity to your KX II-101 unit and Java Runtime Environment v1.4.2_05 or higher installed (JRE is available at <http://java.sun.com/>).
2. Launch a supported web browser such as Internet Explorer (IE) or Firefox.

Launching the KX II-101

3. Type the following URL: `http://IP-ADDRESS`, where IP-ADDRESS is the IP Address that you assigned to your KX II-101 unit. You can also use `https`, the DNS name of the KX II-101 assigned by the administrator (provided that a DNS server has been configured), or just simply type the IP Address in the browser (KX II-101 always redirects the IP Address from HTTP to HTTPS.) The Login page opens:



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

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 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 save the setting.

➤ *To define a direct port access URL:*

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

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

The format for a direct port access URL is:

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

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

KX II-101 Console Layout

The KX II-101 Remote Console interface provides an HTML (Web-like) interface for configuration and administration, as well as target server list and selection. The options are organized into various tabs.

After successful login, the Port Access page opens, displaying the port, its status, and availability.

Launching the KX II-101

KX II-101 Console Navigation

The KX II-101 Remote Console interface provides many methods for navigation and making your selections.

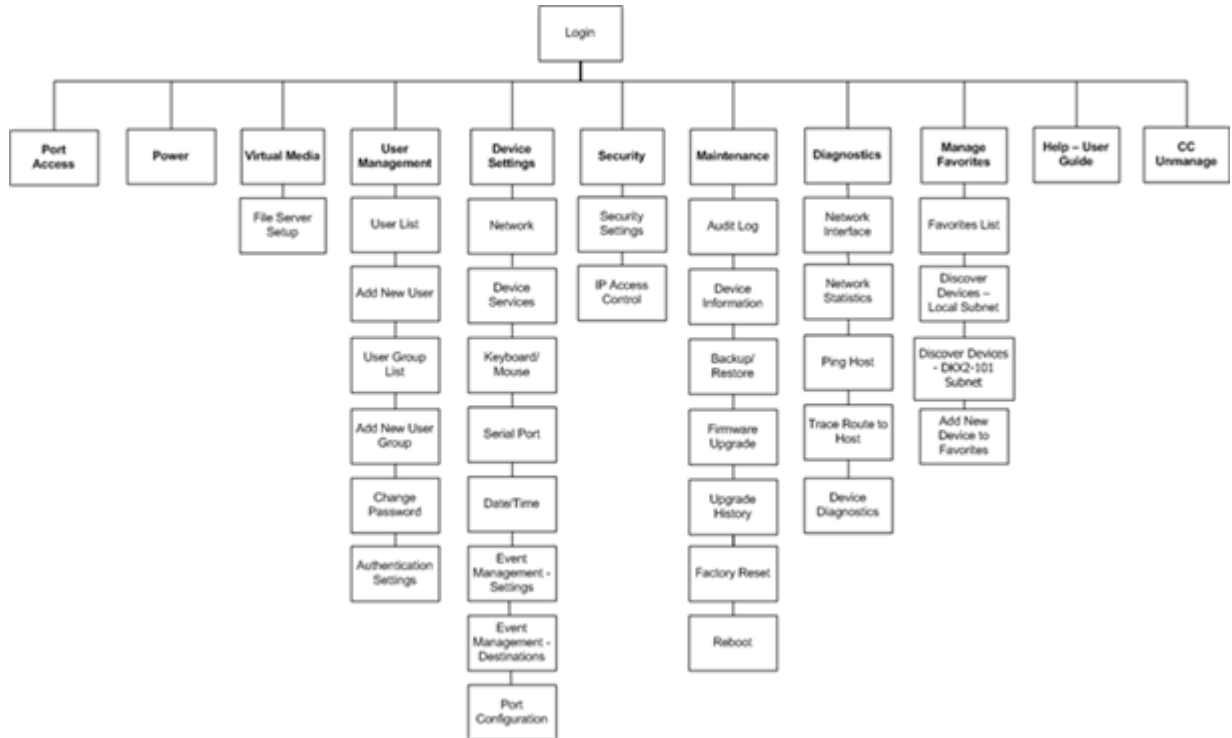
- *To select an option (use any of the following):*
 - Click on a tab; a page of available options is opened.
 - Hover over a tab and select the appropriate option from the menu.
 - Click the option directly from the menu hierarchy displayed (“breadcrumbs”).

Category	Event	SNMP	Syslog	Audit Log
Device Operation	System Startup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Power Supply Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Powerstrip Outlet Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Parameter Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Failure			<input checked="" type="checkbox"/>
	Ethernet Failover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Management	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"/>

- *To scroll through pages longer than the screen:*
 - Use Page Up and Page Down keys on your keyboard, or
 - Use the scroll bar on the right

KX II-101 Remote Console Menu Map

The following diagram represents all of the menu options available in the KX II-101 Remote Console:



Logging Out

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

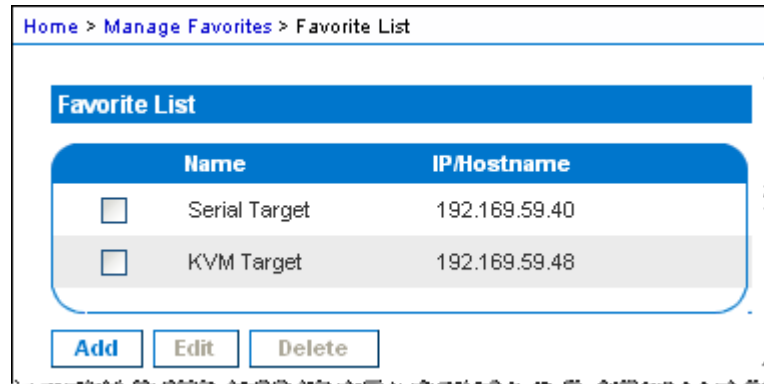
- Click Logout in the upper right-hand corner of the page.

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

Managing Favorites

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

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



- *To access a favorite KX II-101 device:*
 - Click the device name for that device (listed beneath Favorite Devices). A new browser opens to that device.
- *To toggle the Favorite Devices list display between name and IP Address:*

To display Favorites by IP Address:

Click the Display by IP button.

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



To display Favorites by name:

Click the Display by Name button.

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



Manage Favorites Menu

- *To open the Manage Favorites menu:*
 - Click the Manage button. The Manage Favorites page opens and contains the following:

Use:	To:
Favorites List	Manage your list of favorite devices.
Discover Devices - Local Subnet	Discover the devices on the local subnet.
Discover Devices - KX II-101 Subnet	Discover the 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

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:

Favorite List		
	Name	IP/Hostname
<input type="checkbox"/>	KVM Target	192.169.59.48
<input type="checkbox"/>	Serial Target	192.169.59.40
<div><button>Add</button><button>Edit</button><button>Delete</button></div>		

➤ *To add a Favorite:*

- Click the Add button. The *Add New Favorite* (on page 45) page opens.

➤ *To delete a Favorite:*

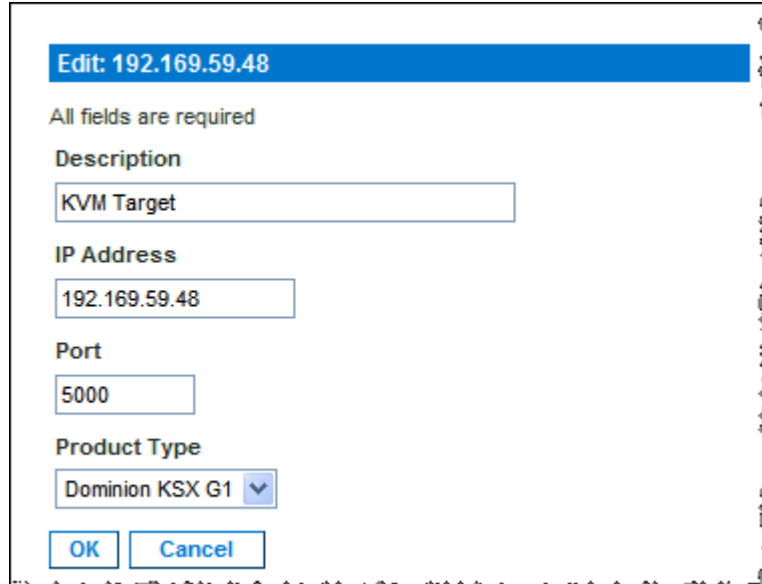
Important: Exercise caution in the removal of favorites; you are not prompted to confirm their deletion.

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

➤ *To edit a Favorite:*

1. From the Favorites List page, select the checkbox next to the appropriate KX II-101 device.

2. Click the Edit button. The Edit page opens:



Edit: 192.169.59.48

All fields are required

Description

KVM Target

IP Address

192.169.59.48

Port

5000

Product Type

Dominion KSX G1 ▼

OK **Cancel**

3. Update the fields as necessary:
 - Description. Type something meaningful.
 - IP Address. Type the IP Address of the KX II-101 unit.
 - Port. Change the discovery Port (if necessary).
 - Product Type.
4. Click OK.

Discover Devices - Local Subnet

This option discovers the devices on your local subnet (that is, the subnet where the KX II-101 Remote Console is running); access these devices directly from this page, or add them to your list of favorites.

Name	IP/Hostname
<input type="checkbox"/> DKX2-101	192.168.50.68
<input type="checkbox"/> KX_KIM-0050	192.168.50.12
<input type="checkbox"/> shoalb-sx	192.168.50.239
<input type="checkbox"/> shoalbkx2	192.168.50.234

➤ *To discover devices on the local subnet:*

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

➤ *To add devices to your Favorites List:*

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

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

➤ *To access a discovered device:*

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

Discover Devices - KX II-101 Subnet

This option discovers the devices on the device subnet (that is, the subnet of the KX II-101 device IP address itself); access these devices directly from this page, or add them to your list of favorites.

This feature allows multiple KX II-101 units to interoperate and scale automatically. The KX II-101 Remote Console automatically discovers the KX II-101 units in the subnet of the KX II-101.

Home > Manage Favorites > Discover Devices - wwwDKX2-101-250 Subnet

Discover Devices - wwwDKX2-101-250 Subnet

Name	IP/Hostname
<input type="checkbox"/> Anil-KSX	192.168.59.193
<input type="checkbox"/> Annette_KSX188	192.168.59.228
<input type="checkbox"/> basker-ksx	192.168.59.250
<input type="checkbox"/> BuilderKX2	192.168.59.75
<input type="checkbox"/> DKSXII	192.168.59.227
<input type="checkbox"/> DKX2-101-TEST	192.168.59.80
<input type="checkbox"/> DKX201GA	192.168.59.21
<input type="checkbox"/> DKX2464-206GA	192.168.59.146
<input type="checkbox"/> DKXSG2-KSX2-188	192.168.59.218
<input type="checkbox"/> Dominion-KX	192.168.59.8
<input type="checkbox"/> DominionKSX	192.168.59.200
<input type="checkbox"/> DominionKSX	192.168.59.204
<input type="checkbox"/> DominionKSX	192.168.59.205
<input type="checkbox"/> DominionKX	192.168.59.202
<input type="checkbox"/> DominionKX	192.168.59.247
<input type="checkbox"/> JaviersBox	192.168.59.249
<input type="checkbox"/> kx2-101_vpn_tes	192.168.59.147
<input type="checkbox"/> LarsKX101	192.168.59.206
<input type="checkbox"/> Ira-ksx2	192.168.59.207
<input type="checkbox"/> sai-KX101	192.168.59.34
<input type="checkbox"/> SE_KX2	192.168.59.53
<input type="checkbox"/> vj	192.168.59.224
<input type="checkbox"/> wwwDKX2-101-250	192.168.59.140

Select All
Deselect All

Add
Refresh

Copyright © 2007 Raritan Computer Inc.

➤ *To discover devices on the device subnet:*

1. Choose Favorites > Discover Devices - KX II-101 Subnet. The Discover Devices - KX II-101 Subnet page opens.
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.

Add New Favorite

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

1. Choose Manage Favorites > Add New Device to Favorites. The Add New Favorite page opens:
2. Type a meaningful description.
3. Type the IP Address for the device.
4. Change the discovery Port (if necessary).
5. Click OK.

This device is added to your list of favorites.

Port Access Page

After successfully logging into the KX II-101 Remote Console, the Port Access page opens. This page displays the KX II-101 port, 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 you want to control through the KX II-101 unit; it is connected to the KX II-101 using the attached PS/2 connectors on the device.

Note: For each connection to a KVM target server, a new Virtual KVM Client window is opened.

➤ *To use the Port Access page:*

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

No.	Name	Availability
1	Dominion_KX2_101_Port5	idle

- No. There is just one port available for the KX II-101.
 - Name. The name of the KX II-101 port; initially set to Dominion_KX101G2_Port1, but you can change the name to something more descriptive.
 - Availability. The Availability can be Idle, Connected, Busy, or Unavailable.
2. To connect to the target server, click the Name of the device/target server then click the Connect pop-up. The Virtual KVM Client window opens and the availability changes to Busy.
 3. To disconnect from the target server, click the Name of the device/target server then click the Disconnect pop-up. The Virtual KVM Client window closes and the availability changes to Idle.

Chapter 5 Users, Groups, and Access Permissions

In This Chapter

Users	47
Groups.....	47
Relationship between Users and Groups	48
User Management.....	49
Remote Authentication	61

Users

The KX II-101 stores an internal list of all user and group names to determine access authorization and permissions. This information is stored internally in an encrypted format. There are several forms of authentication and this one is known as “local authentication”. All users have to be authenticated; if KX II-101 is configured for LDAP/LDAPS or RADIUS, that authentication is processed first, followed by local authentication.

User names and passwords are required to gain access to the KX II-101 unit. This information is used to authenticate users attempting to access your KX II-101 unit. Refer to User Management for more information about adding and editing users.

Groups

Every KX II-101 unit is delivered with three default user groups; these groups cannot be deleted:

Admin	Users that are a member of this group have full administrative privileges. The original, factory-default user is a member of this group and has the complete set of system privileges. In addition, the Admin user must be a member of the Admin group.
-------	---

Relationship between Users and Groups

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

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

Relationship between Users and Groups

Users belong to a group and groups have privileges. Organizing the various users of your 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 - which server ports are accessible, whether rebooting the unit is allowed, and other features.

User Management

User Management Menu

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

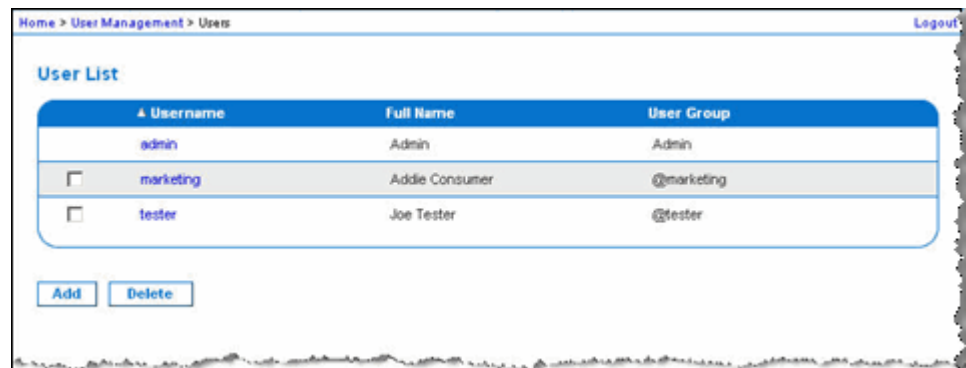
Use:	To:
User List	Display an alphabetical list of all users; add, modify, or delete users.
Add New User	Add new users; modify user information.
User Group List	Display an alphabetical list of all user groups; add, modify, or delete user groups.
Add New User Group	Add new user groups; modify user group information.
Change Password	Change password for a specific user.
Authentication Settings	Configure the type of authentication used for access to the KX II-101.

User List

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

➤ *To view the list of users:*

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



User Management

➤ *To add a new user:*

- Click the Add button. The User page opens. For complete information about the User page, refer to **Add New User** (on page 50).

➤ *To modify an existing user:*

1. Locate the user from among those listed.
2. Click on the Username. The User page opens. For complete information editing the user, refer to **Modify Existing User** (on page 52).

➤ *To delete a user:*

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

Add New User

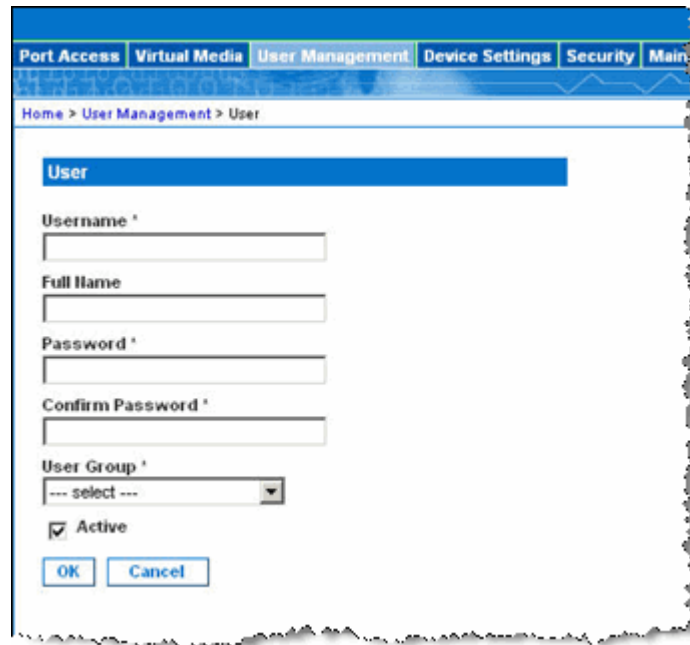
It is a good idea to define user groups before creating KX II-101 users, because when you add a user, you must assign that user to an existing user group. From the User page, you can add new users, modify user information, and reactivate users that have been deactivated.

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

➤ *To add a new user:*

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

- Click the Add button from the User List page

The screenshot shows a web interface for user management. At the top, there are tabs for 'Port Access', 'Virtual Media', 'User Management', 'Device Settings', 'Security', and 'Main'. Below the tabs is a breadcrumb trail: 'Home > User Management > User'. The main content area is titled 'User' and contains several input fields: 'Username *', 'Full Name', 'Password *', 'Confirm Password *', and 'User Group *'. The 'User Group *' field is a drop-down menu with '--- select ---' as the current selection. Below these fields is a checkbox labeled 'Active' which is checked. At the bottom of the form are 'OK' and 'Cancel' buttons.

2. Type a unique name in the Username field (up to 16 characters).
3. Type the person's full name in the Full Name field (up to 64 characters).
4. Type a password in the Password field; retype the password in the Confirm Password field (up to 64 characters).
5. Choose the group from the User Group drop-down list. The list contains all groups you have created in addition to the system-supplied default groups (<Unknown> (default setting), Admin, Individual Group). If you do not want to associate this user with an existing User Group, choose Individual Group from the drop-down list.

Note: The Admin user must be a member of the Admin group.

For more information about permissions for an Individual Group, refer to *Set Permissions for Individual Group* (on page 56).

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

User Management

Modify Existing User

➤ *To modify an existing user:*

1. In the User page, change the appropriate fields. (Refer to *Add New User* (on page 50) for information about how to get access the User page.)
2. 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 147) for information. A blocked user becomes inactive and can be unblocked by being made active again by the administrator.

➤ *To block or unblock a user:*

1. Chooser User Management > User.
The User page appears.
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.

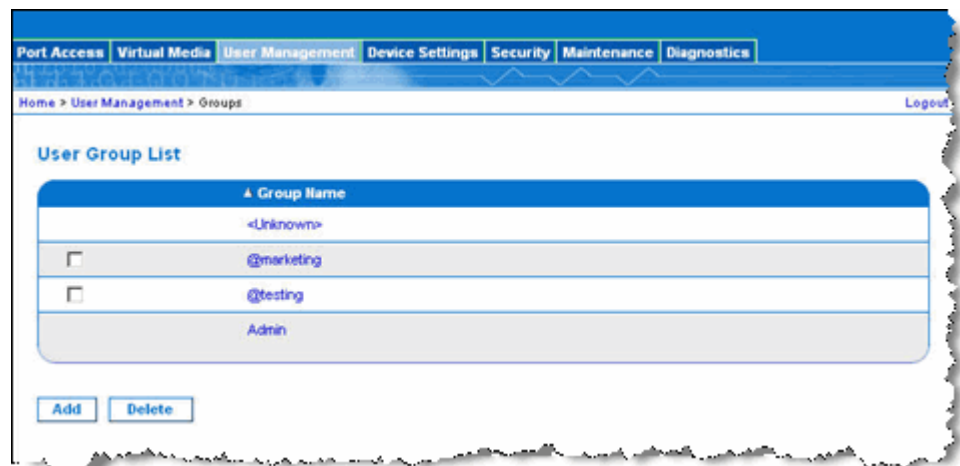
User Group List

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

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

➤ *To list the user groups:*

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



➤ *To add a new user group:*

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

➤ *To modify an existing user group:*

1. Locate the user group from among those listed.
2. Click on the Group Name. The Group page opens. For complete information editing the group, refer to *Modify Existing User Group* (on page 59).

➤ *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.

User Management

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

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

Add New User Group

➤ *To add a new user group:*

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

The screenshot shows the 'Group' configuration page. At the top is a breadcrumb trail: 'Home > User Management > Group'. Below this is a blue header bar labeled 'Group'. Underneath is a 'Group Name' field with a small asterisk and a text input box. A blue bar labeled 'Permissions' with a dropdown arrow contains a list of checkboxes for 'Device Settings', 'Diagnostics', 'Maintenance', 'PC-Share', 'Security', and 'User Management'. Below that is another blue bar labeled 'Port Permissions' with a dropdown arrow. This section contains a table with four columns: 'Port', 'Access', 'VM Access', and 'Power Control'. The 'Port' column lists 'Dominion_KX2_101_Port1' and 'Power Port 1'. The 'Access' column has a 'Deny' dropdown. The 'VM Access' column has a 'Deny' dropdown. The 'Power Control' column has a 'Deny' dropdown. Below the table is a blue bar labeled 'IP ACL' with a dropdown arrow. This section contains a table with four columns: 'Rule #', 'Starting IP', 'Ending IP', and 'Action'. The 'Action' column has a dropdown menu currently set to 'ACCEPT'. Below the table are four buttons: 'Append', 'Insert', 'Replace', and 'Delete'. At the bottom left are 'OK' and 'Cancel' buttons.

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.

3. Set the Permissions for the group. Select the checkboxes before the permissions you want to assign to all of the users belonging to this group. Refer to *Setting Permissions* (on page 55) for more information.
4. Set the Port Permissions. Specify the type of access to give to the KVM and power port. Refer to Setting Port Permissions for more information.
5. Set the IP ACL (optional). This feature limits access to the KX II-101 device by specifying IP addresses; it applies only to users belonging to a specific group, unlike the *IP Access Control* (on page 151) list feature which applies to all access attempts to the device (and takes priority).
6. Click OK.

Note: Several administrative functions are available within MPC; these functions are available only to members of the default ADMIN group.

Setting Permissions

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

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/RADIUS), login settings.

Set Permissions for Individual Group

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

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

Setting Port Permissions

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

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

* Default setting

Group-based IP ACL (Access Control List)

Important: Please exercise caution when using group-based IP access control. It is possible to be locked out of your 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 which applies to all access attempts to the device, is processed first, and takes priority. Refer to *IP Access Control* (on page 151) for more information.

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

➤ *To add (append) rules:*

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

➤ *To insert a rule:*

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

4. Click Insert. If the Rule # you just typed equals an existing Rule #, the new rule is placed ahead of the exiting rule and all rules are moved down in the list.

➤ *To replace a rule:*

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

➤ *To delete a rule:*

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

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

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

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

Modify Existing User Group

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

➤ *To modify an existing user group:*

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

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
Dominion_KX2_101_Port1	Deny	Deny	Deny
Power Port 1	Deny		Deny

IP ACL

Rule #	Starting IP	Ending IP	Action
			ACCEPT

Append Insert Replace Delete

OK Cancel

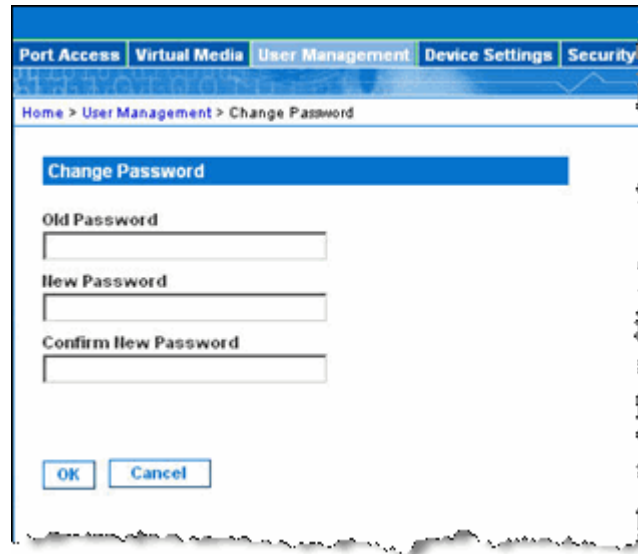
2. Set the Permissions for the group. Select the checkboxes before the permissions you want to assign to all of the users belonging to this group. Refer to *Setting Permissions* (on page 55) for more information.
3. Set the Port Permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). Refer to *Setting Port Permissions* for more information.
4. Set the IP ACL (optional). This feature limits access to the KX II-101 device by specifying IP addresses. Refer to *Group-based IP Access Control List* for more information.
5. Click OK.

User Management

Change Password

➤ *To change your password:*

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

The screenshot shows a web interface with a blue header bar containing tabs for 'Port Access', 'Virtual Media', 'User Management', 'Device Settings', and 'Security'. Below the header, a breadcrumb trail reads 'Home > User Management > Change Password'. The main content area has a blue title bar labeled 'Change Password'. Below this, there are three text input fields labeled 'Old Password', 'New Password', and 'Confirm New Password'. At the bottom of the form are two buttons: 'OK' and 'Cancel'.

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

Note: If strong passwords are in use, this page displays information about the format required for the passwords. For more information about passwords and strong passwords, refer to *Security Settings - Strong Passwords* (see "Strong Passwords" on page 146).

Authentication Settings

Authentication settings are described in the discussion of remote authentication later in this chapter. See Authentication Settings for information.

Remote Authentication

Note to CC-SG Users

When the KX II-101 is controlled by CommandCenter Secure Gateway, CC-SG authenticates users and groups, except for local users (requiring local port access). When CC-SG is controlling the KX II-101, local port users will be authenticated against the local user database or the Remote Authentication server (LDAP/LDAPS or RADIUS) configured on the KX II-101; they will not be authenticated against the CC-SG user database.

For additional information about CC-SG authentication, refer to the CommandCenter Secure Gateway User Guide, Administrator Guide, or Deployment Guide at:

<http://www.raritan.com/support/productdocumentation>.

Supported Protocols

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

Note on Microsoft Active Directory

Microsoft Active Directory uses the LDAP/LDAPS protocol natively, and can function as an LDAP/LDAPS server and authentication source for 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.

Authentication vs. Authorization

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

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

Authentication Settings

From the Authentication Settings page you can configure the type of authentication used for access to your KX II-101. Refer to *Authentication vs. Authorization* (on page 61) for more information about how authentication and authorization operate and differ.

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

➤ *To configure authentication:*

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

The screenshot shows the 'Authentication Settings' page. At the top, there's a breadcrumb trail: 'Home > User Management > Authentication Settings'. Below this is a tab labeled 'Authentication Settings'. The page is divided into two main sections: 'Local Authentication' and 'Remote Authentication'. Under 'Local Authentication', there are radio buttons for 'Local Authentication' (selected) and 'LDAP'. Below these are fields for 'Primary LDAP Server', 'Secondary LDAP Server', 'Secret Phrase', 'Confirm Secret Phrase', and a checkbox for 'Enable Secure LDAP'. There are also fields for 'Port' (200), 'Secure LDAP Port' (636), 'Certificate File' (with a 'Browse...' button), 'DN of Administrative User', 'User Search DN', and 'Type of External LDAP Server' (set to 'Generic LDAP server'). Under 'Remote Authentication', there are radio buttons for 'RADIUS' (selected) and 'LDAP'. Below these are fields for 'Primary RADIUS Server', 'Shared Secret', 'Authentication Port' (1812), 'Accounting Port' (1813), 'Timeout (in seconds)' (1), 'Retries' (3), 'Secondary RADIUS Server', 'Shared Secret', 'Authentication Port' (1812), 'Accounting Port' (1813), 'Timeout (in seconds)' (1), and 'Retries' (3). At the bottom, there's a 'Global Authentication Type' dropdown set to 'RADIUS'. At the very bottom are three buttons: 'OK', 'Reset To Defaults', and 'Cancel'.

2. Choose the option for the authentication protocol you want to use (Local Authentication, LDAP, 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, read the section entitled Implementing LDAP Remote Authentication for information about completing the fields in the LDAP section of the Authentication Settings page.
 5. If you choose RADIUS, read the section entitled ***Implementing RADIUS Remote Authentication*** (on page 67) for information about completing the fields in the RADIUS section of the Authentication Settings page.
 6. Click OK to save.
- *To cancel without saving changes:*
- Click Cancel.
- *To return to factory defaults:*
- Click the Reset to Defaults button.

Remote Authentication

Implementing LDAP Remote Authentication

Lightweight Directory Access Protocol (LDAP) 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 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 authentication server.

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

1. Type the IP Address or DNS name of your LDAP remote authentication server in the Primary LDAP Server field. When the Enable Secure LDAP option is checked, the DNS name must be used.

2. (Optional) Type the IP Address or DNS name of your backup LDAP server in the Secondary LDAP Server field. When the Enable Secure LDAP option is selected, the DNS name must be used. Please note that the remaining fields share the same settings with the Primary LDAP Server field.
3. Type the server secret (password) required to authenticate against your remote authentication server in the Secret Phrase field and again in the Confirm Secret Phrase field. Do not change the existing schema. Use the string in use on the LDAP server.
4. Select the Enable Secure LDAP checkbox if you would like to use SSL; the Secure LDAP Port field is enabled. Secure Sockets Layer (SSL) is a cryptographic protocol which allows KX II-101 to communicate securely with the LDAP server.
5. The default Port is 389. Either use the standard LDAP TCP port or specify another port.
6. The default Secure LDAP Port is 636. Either use the default port or specify another port. This field is enabled when the Enable Secure LDAP checkbox is selected.
7. Certificate File. Consult your authentication server administrator to get the CA certificate file in Base64 encoded X-509 format for the LDAP server. Use the Browse button to navigate to the certificate file. This field is enabled when the Enable Secure LDAP option is checked.
8. DN of administrative User. Distinguished Name of administrative user; consult your authentication server administrator for the appropriate values to type into this field. An example DN of administrative User value might be:
"cn=Administrator,cn=Users,dc=testradius,dc=com".
9. User Search DN. This describes the name you want to bind against the LDAP, and where in the database to begin searching for the specified Base DN. An example Base Search value might be:
"cn=Users,dc=raritan,dc=com". Consult your authentication server administrator for the appropriate values to enter into these fields.
10. Type of external LDAP server. Choose from among the options available:
 - Generic LDAP Server.
 - Microsoft Active Directory. Active Directory is an implementation of LDAP directory services by Microsoft for use in Windows environments.

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

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).

Note: If you are an existing Raritan, Inc. customer, and have already configured the Active Directory server by changing the AD schema, KX II-101 still supports this configuration, and you do not need to perform the following operations. Please refer to *Updating the LDAP Schema* (on page 69) for information about updating the AD LDAP schema.

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

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

Important Notes:

- Group Name is case sensitive.
- The KX II-101 provides the following default groups which can not be changed or deleted: Admin and <Unknown>. Please verify that your Active Directory server does not use the same group names.
- If the group information returned from the Active Directory server does not match a 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:*

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

1. Type the IP Address of your primary and (optional) secondary remote authentication servers in the Primary Radius Server and Secondary Radius Server fields, respectively.
2. Type the server secret used for authentication (in the Shared Secret fields). The shared secret is a character string that must be known by both the KX II-101 and the RADIUS server to allow them to communicate securely. It is essentially a password.
3. Authentication Port. The default authentication port is 1812; change as required.

Remote Authentication

4. Accounting Port. The default accounting port is 1813; change as required.
5. Timeout (in seconds). The default timeout is 1 second; change as required. The timeout is the length of time the KX II-101 waits for a response from the RADIUS server before sending another authentication request.
6. Retries. The default number of retries is 3; change as required. This is the number of times the KX II-101 will send an authentication request to the RADIUS server.
7. Global Authentication Type. Choose from among the options in the drop-down list:
 - PAP. With PAP, passwords are sent as plain text. PAP is not interactive; the username and password are sent as one data package once a connection is established, rather than the server sending a login prompt and waiting for a response.
 - CHAP. With CHAP authentication can be requested by the server at any time. CHAP provides more security than PAP.

Returning User Group Information via RADIUS

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

Your remote RADIUS server can provide these user group names by returning an attribute, implemented as a RADIUS FILTER-ID. The FILTER-ID should be formatted as follows:

Raritan:G{GROUP_NAME}

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 unit sends the following RADIUS attributes to your RADIUS server:

Attribute	Data
Login	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) for network connections.

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

Updating the LDAP Schema

Note: The procedures in this chapter should be attempted only by experienced users.

Returning User Group Information

Use the information in this chapter to return User Group information (and assist with authorization) once authentication is successful.

Remote Authentication

From LDAP

When an LDAP/LDAPS authentication is successful, KX II-101 determines the permissions for a given user based on the permissions of the user's group. Your remote LDAP server can provide these user group names by returning an attribute named as follows:

rciusergroup attribute type: string

This may require a schema extension on your LDAP/LDAPS server. Consult your authentication server administrator to enable this attribute.

From Microsoft Active Directory

Note: This should be attempted only by an experienced Active Directory administrator.

Returning user group information from Microsoft's Active Directory for Windows 2000 Server requires updating the LDAP/LDAPS schema. Refer to your Microsoft documentation for more detail.

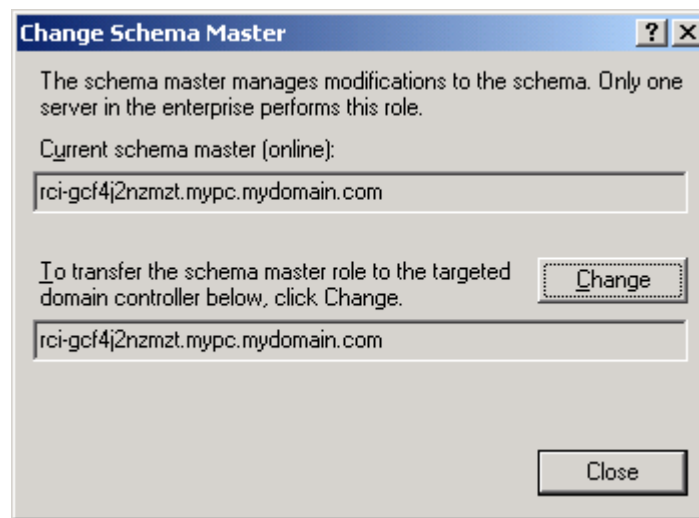
1. Install the schema plug-in for Active Directory - refer to Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

➤ *To permit write operations to the schema:*

1. Right-click the Active Directory Schema root node in the left pane of the window, and then click Operations Master. The Change Schema Master dialog opens:



2. (Optional) Select the checkbox before The Schema can be modified on this Domain Controller.
3. Click OK.

Creating a New Attribute

➤ *To create new attributes for the rciusergroup class:*

1. Click the + symbol before Active Directory Schema in the left pane of the window.
2. Right-click Attributes in the left pane.

Remote Authentication

- Click New, and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute window opens.

Create New Attribute

Create a New Attribute Object

Identification

Common Name: rciusergroup

LDAP Display Name: rciusergroup

Unique X500 Object ID: 1.3.6.1.4.1.13742.50

Description: Raritan's LDAP attribute

Syntax and Range

Syntax: Case Insensitive String

Minimum: 1

Maximum: 24

☐ Multi-Valued

OK Cancel

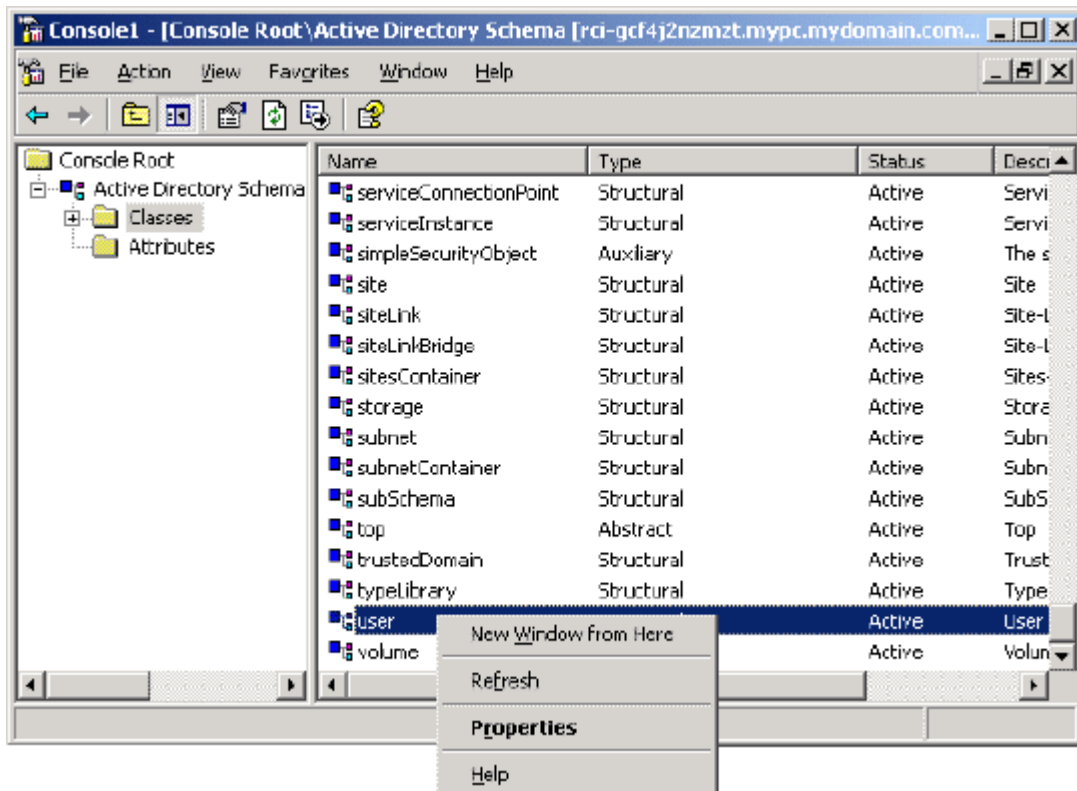
- Type rciusergroup in the Common Name field.
- Type rciusergroup in the LDAP Display Name field.
- Type 1.3.6.1.4.1.13742.50 in the Unique x5000 Object ID field.
- Type a meaningful description in the Description field.
- Click the Syntax drop-down arrow and choose Case Insensitive String from the list.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

Adding Attributes to the Class

➤ *To add attributes to the class:*

- Click Classes in the left pane of the window.

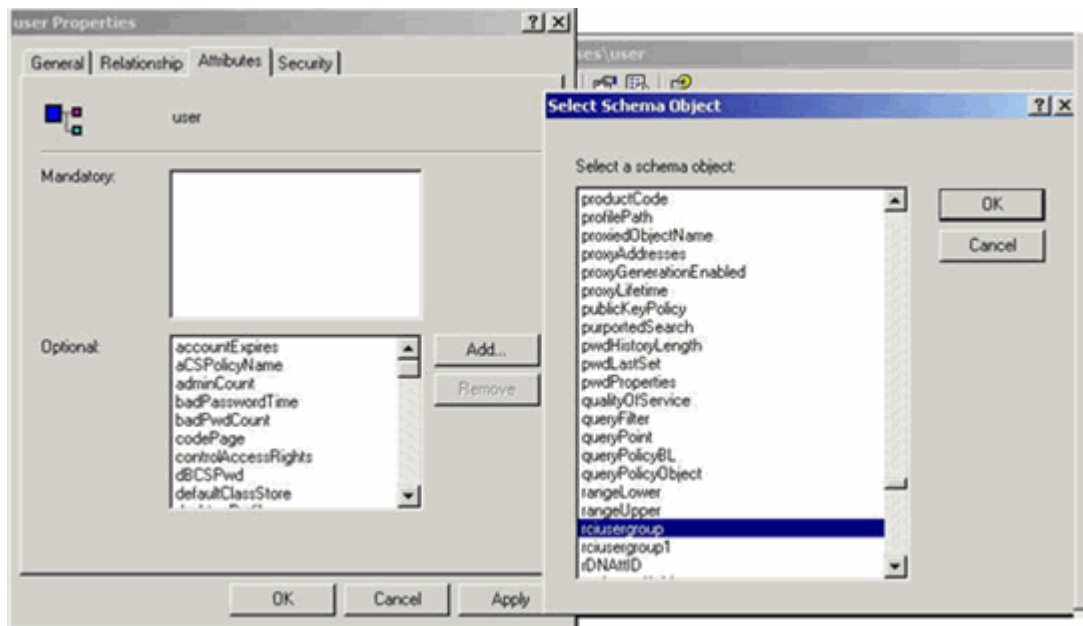
2. Scroll to the user class in the right pane, and right-click on it.



3. Choose Properties from the menu. The user Properties window appears.

Remote Authentication

- Click on the Attributes tab to open it.



- Click Add.
- Choose rcusergroup from the Select Schema Object list.
- Click OK in the Select Schema Object dialog.
- Click OK in the user Properties dialog.

Updating the Schema Cache

➤ *To update the schema cache:*

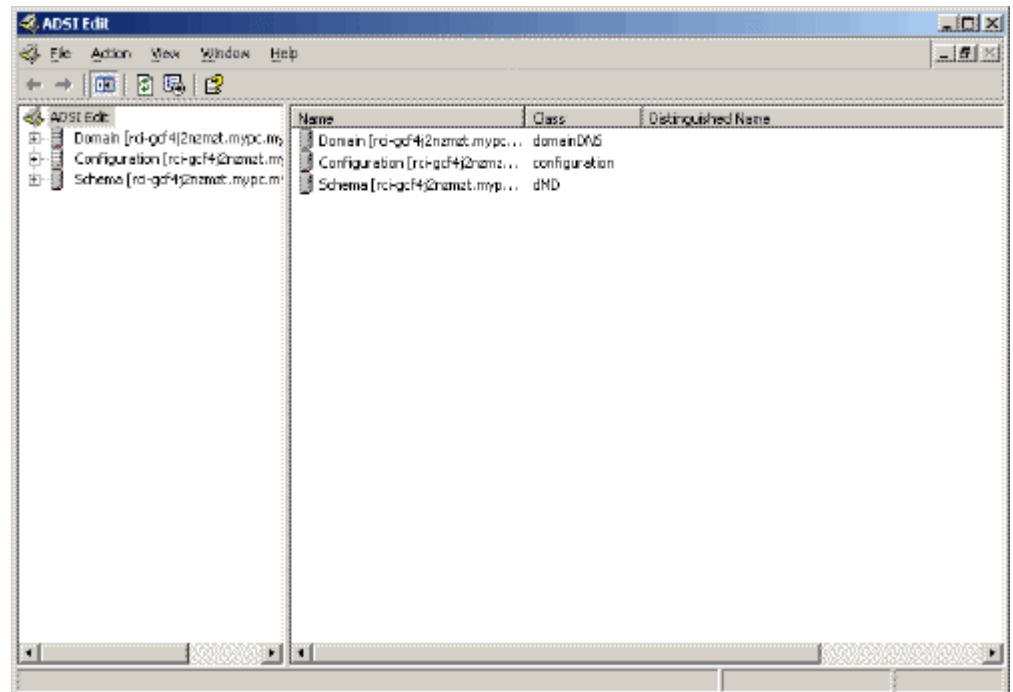
- Right-click Active Directory Schema in the left pane of the window and select Reload the Schema from the shortcut menu.
- Minimize the Active Directory Schema MMC (Microsoft Management Console) console.

Editing rcusergroup Attributes for User Members

To run Active Directory script on Windows 2003 server, please use the script provided by Microsoft (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

➤ *To edit the individual user attributes within the group rcusergroup:*

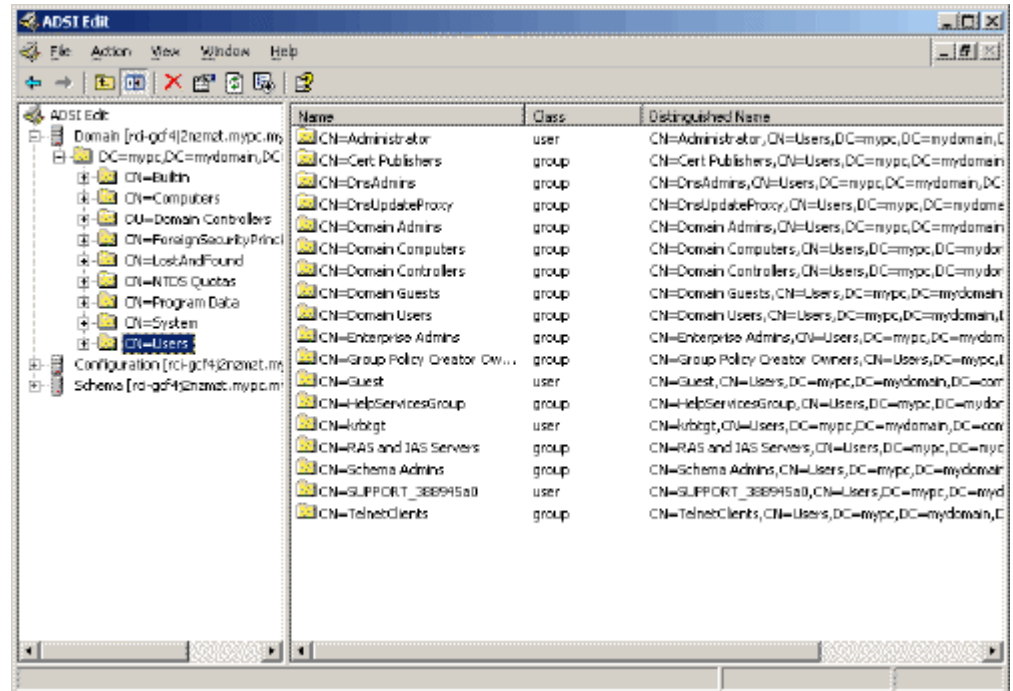
1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.
3. Go to the directory where the support tools were installed.
4. Run adsiedit.msc. The ADSI Edit window opens.



5. Open the Domain.

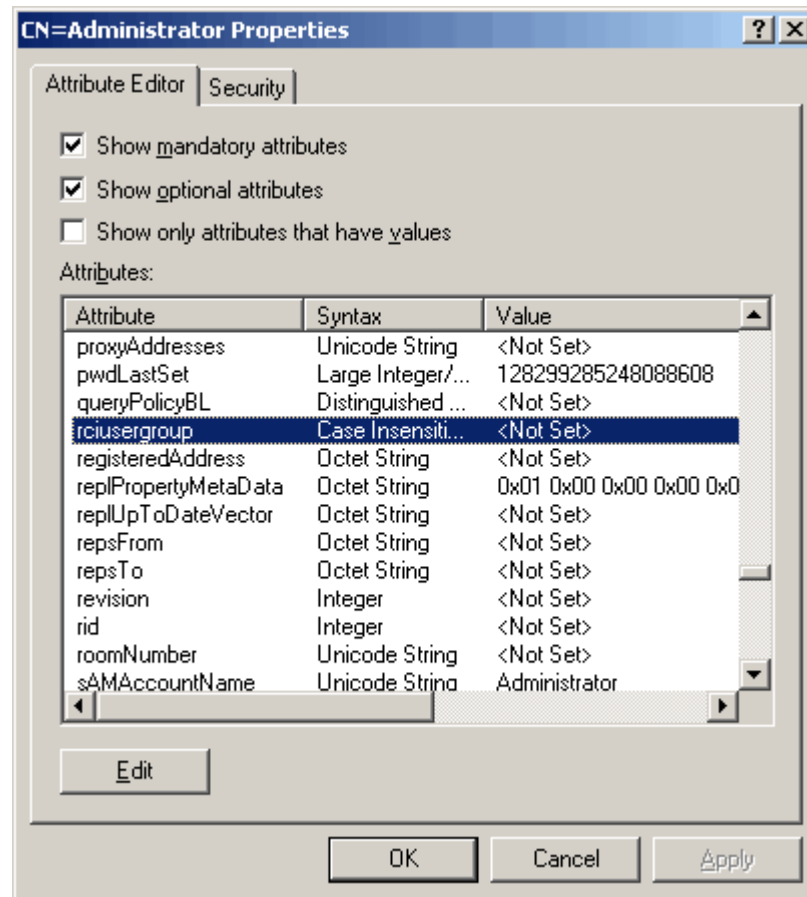
Remote Authentication

6. In the left pane of the window, select the CN=Users folder.



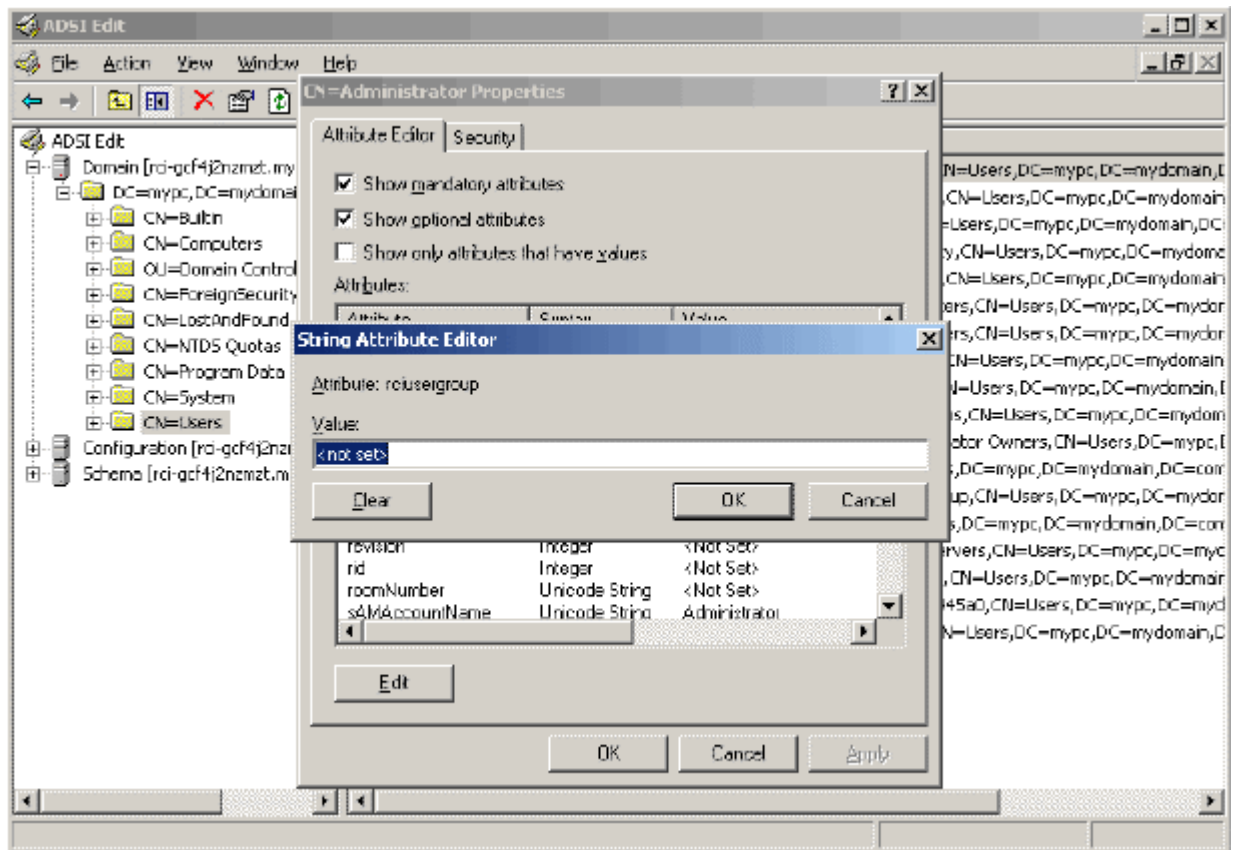
7. Locate the user name whose properties you want to adjust in the right pane. Right-click on the user name and select Properties.
8. Click on the Attribute Editor tab if it is not already open.

9. Choose rcusergroup from the Attributes list.

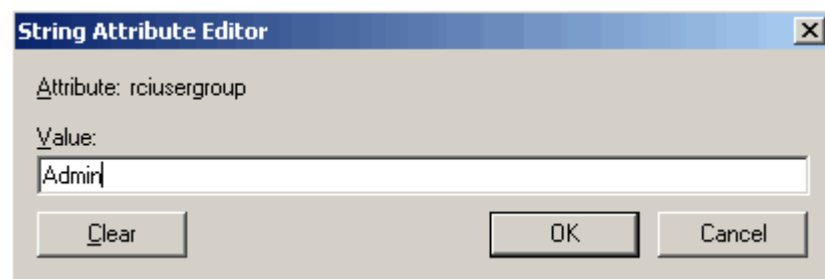


Remote Authentication

10. Click Edit. The String Attribute Editor dialog opens:



11. Type the user group (created in Dominion KX II-101) in the Edit Attribute field.



12. Click OK.

Chapter 6 Virtual KVM Client

In This Chapter

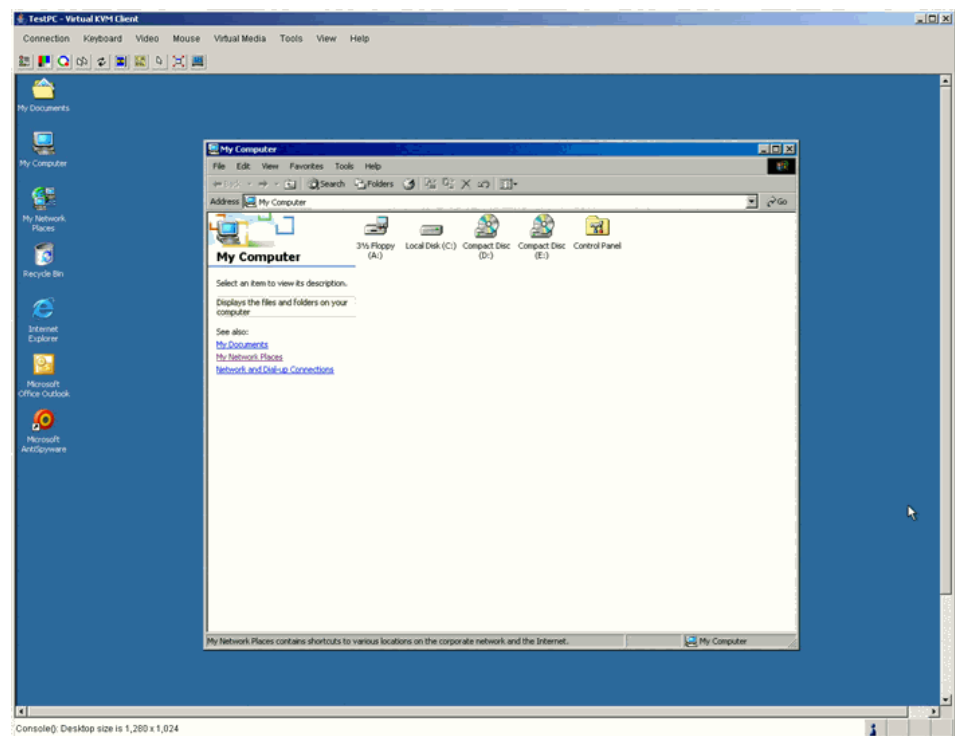
Overview.....	80
Options.....	81
Mouse Pointer Synchronization.....	83
Connection Menu	85
Keyboard Menu	88
Video Menu	92
Mouse Menu.....	96
Virtual Media	98
Tools Menu	99
View Menu	100
Help Menu.....	101

Overview

Whenever you access a target server using the KX II-101 Remote Console, a Virtual KVM Client window is opened.

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

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



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

Feature	Description
Menu Bar	Drop-down menus of commands and settings.
Toolbar	Shortcut buttons to frequently used features and commands.
Target Server Video Window	Target device display.

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

Options

Menu Tree











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

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

Options

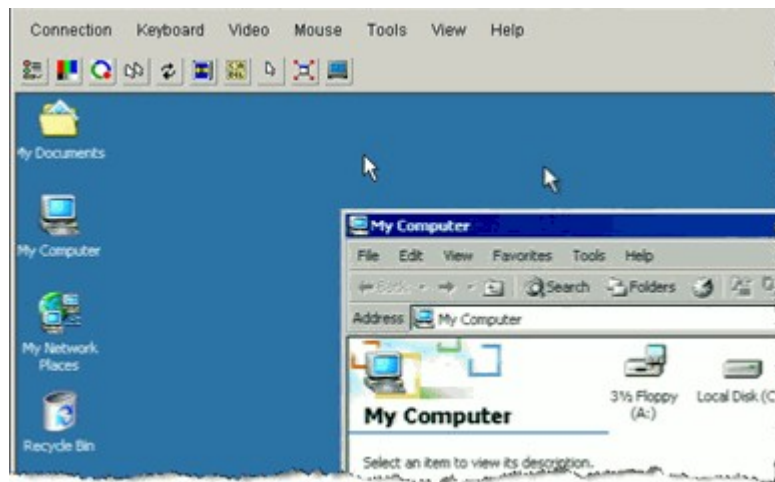
- Connect CD-ROM/ISO Image
- Tools
 - Options
- View
 - View Toolbar
 - Scaling
 - Target Screen Resolution
- Help
 - About Raritan Virtual KVM Client

Toolbar

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

Mouse Pointer Synchronization

When remotely viewing a target server that uses a mouse, you will see two mouse pointers: one belonging to your remote client workstation and the other belonging to the target server. When the mouse pointer lies within the Virtual KVM Client target server window, mouse movements and clicks are directly transmitted to the connected target server. While in motion, the client mouse pointer slightly leads the target mouse pointer due to mouse acceleration settings.




On fast LAN connections, you may want to disable the Virtual KVM Client mouse pointer and view only the target server's pointer. You can toggle between these two modes (single mouse and dual mouse). Refer to *Mouse Menu* (on page 96) for additional information about the available mouse modes.

Mouse Synchronization Tips

Be sure to follow these steps when obtaining mouse synchronization:

1. Verify that the selected video resolution and refresh rate is among those supported by the KX II-101. The Virtual KVM Client Connection Info dialog displays the actual values that the KX II-101 is seeing. Please refer to Supported Video Resolutions for more information about the video resolutions that are supported.
2. Verify that the cable length is within the specified limits for the selected video resolution. Please refer to Target Server Connection Distance and Video Resolution for more information.

Mouse Pointer Synchronization

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


Additional Notes for Intelligent Mouse Mode

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

Connection Menu

Properties Dialog

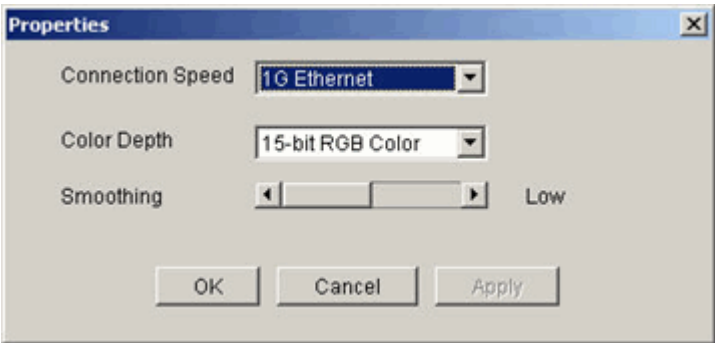
The KX II-101 dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. KX II-101 units optimize KVM output not only for LAN use, but also for WAN use. These units can also control color depth and limit video output, offering an optimal balance between video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

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

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

➤ *To set the connection properties:*

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



2. Choose the Connection Speed from the drop-down list. KX II-101 can automatically detect available bandwidth and not limit bandwidth use; but you can also adjust this usage according to bandwidth limitations.

- Auto
- 1G Ethernet
- 100 Mb Ethernet
- 10 Mb Ethernet
- 1.5 Mb (MAX DSL/T1)
- 1 Mb (Fast DSL/T1)
- 512 Kb (Medium DSL/T1)

Connection Menu

384 Kb (Slow DSL/T1)

256 Kb (Cable)

128 Kb (Dual ISDN)

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

3. Choose the Color Depth from the drop-down list. KX II-101 can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths.

15-bit RGB Color

8-bit RGB Color

4-bit Color

4-bit Gray

3-bit Gray

2-bit Gray

Black and White

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

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.

➤ *To cancel without saving changes:*

- Click Cancel.

Connection Info

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

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

The following information is displayed about the current connection:

- Device Name. The name of the KX II-101 device.
- IP Address. The IP Address of the KX II-101 device.
- Port. The KVM Communication TCP/IP Port used to access the target device.
- Data In/Second. Data rate in.
- Data Out/Second. Data rate out.
- Connect Time. The duration of the connect time.
- FPS. The frames per second transmitted for video.
- Horizontal Resolution. The screen resolution horizontally.
- Vertical Resolution. The screen resolution vertically.
- Refresh Rate. How often the screen is refreshed.
- Protocol Version. RFB Protocol version.

➤ *To copy this information:*

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

Exit

➤ *To close the Virtual KVM Client (the target you are currently accessing):*


- Choose Connection > Exit.

Keyboard Menu

Send Ctrl+Alt+Delete

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

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

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

➤ *To send a Ctrl+Alt+Delete key sequence to the target server:*

- Choose Keyboard > Send Ctrl+Alt+Delete, or
- Click the Send Ctrl+Alt+Delete button from toolbar

Keyboard Macros

Keyboard macros ensure that keystroke combinations intended for the target server, are sent to and interpreted only by the target server. Otherwise, they might be interpreted by the computer on which the Virtual KVM Client is running (your client PC).

Macros are stored on the client PC and are PC-specific; therefore, if you use another PC you will not see your macros. In addition, if another person uses your PC and logs in under a different name, that user will see your macros since they are computer-wide. Keyboard macros created in the Virtual KVM Client are available in MPC and vice versa.

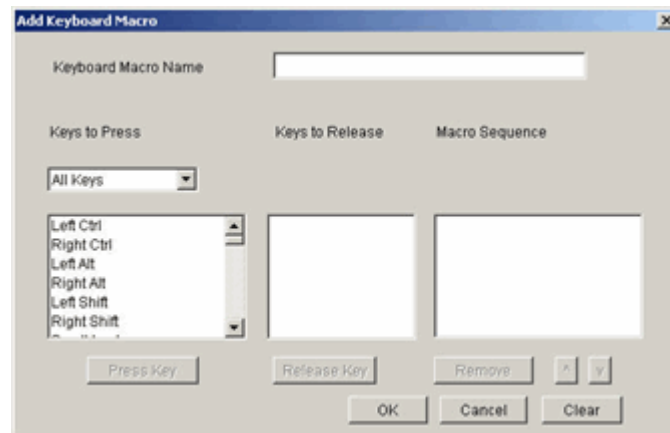
Creating a Keyboard Macro

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

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



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



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

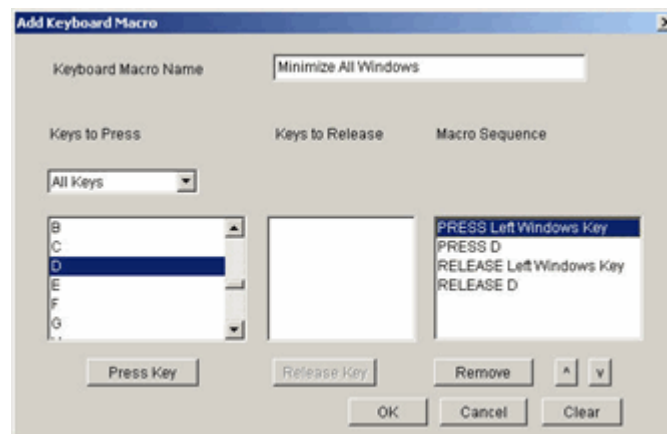
Keyboard Menu

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

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

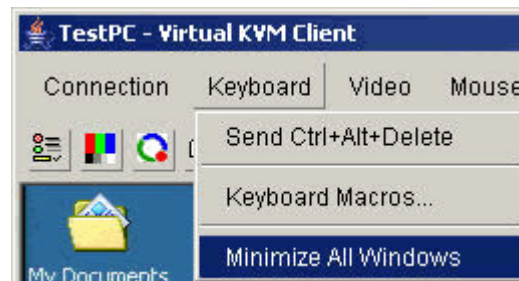
In this example, both keys pressed must also be released.

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



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

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



➤ *To cancel without saving changes:*

- Click Cancel.

➤ *To clear all fields and start over:*

- Click the Clear button.

Running a Keyboard Macro

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

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

- Choose Keyboard > Minimize All Windows.

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

➤ *To execute a macro:*

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

Modifying a Keyboard Macro

➤ *To modify a macro:*

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

Removing a Keyboard Macro

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

Video Menu

➤ *To remove a macro:*

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

Video Menu

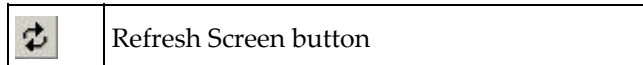
Video settings can be refreshed automatically in several ways:

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

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

Refresh Screen

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



➤ *To refresh the video settings:*

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

Auto-sense Video Settings

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




➤ *To automatically detect the video settings:*

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

A message is displayed that auto adjustment is in progress.

Calibrate Color

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

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

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

➤ *To calibrate the color:*

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

Video Settings

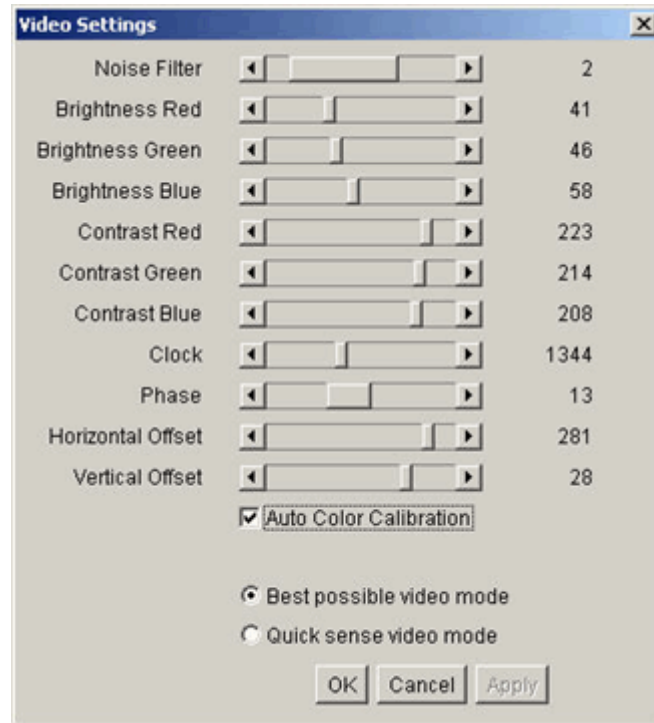
Use the Video Settings option to manually adjust the video settings.

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

Video Menu

➤ *To change the video settings:*

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



2. Use the sliders to adjust the settings to achieve the desired results (as you adjust the settings the effects are immediately visible):
 - Noise Filter. KX II-101 can filter out the electrical interference of video output from graphics cards. This feature optimizes picture quality and reduces bandwidth. Higher settings transmit variant pixels only if a large color variation exists in comparison to the neighboring pixels. However, setting the threshold too high can result in the unintentional filtering of desired screen changes. Lower settings transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.
 - Brightness: Use this setting to adjust the brightness of the target server display.
 - Red. Controls the brightness of the red signal.
 - Green. Controls the brightness of the green signal.
 - Blue. Controls the brightness of the blue signal.
 - Color Contrast Settings: Controls the contrast adjustment.

- Contrast Red. Controls the red signal.
- Contrast Green. Controls the green signal.
- Contrast Blue. Controls the blue signal.
- If the video image looks extremely blurry or unfocused, the settings for clock and phase can be adjusted until a better image appears on the active target server.

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

- Clock. Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally; odd number settings are recommended. Under most circumstances this setting should not be changed because the auto-detect is usually quite accurate.
 - Phase. Phase values range from 0 to 31 and will wrap around. Stop at the phase value that produces the best video image for the active target server.
 - Offset: Controls the on-screen positioning:
 - Horizontal Offset. Controls the horizontal positioning of the target server display on your monitor.
 - Vertical Offset. Controls the vertical positioning of the target server display on your monitor.
 - Auto Color Calibration. Check this option if you would like automatic color calibration.
 - Video Sensing: Select the video sensing mode:
 - Best possible video mode: KX II-101 will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.
 - Quick sense video mode: With this option, the KX II-101 will use a quick video Auto Sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.
3. Click Apply. The Video Settings are changed.

Mouse Menu

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

- *To cancel with saving your changes:*
 - Click Cancel.

Mouse Menu

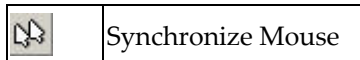
When controlling a target server, the KX II-101 Remote Console displays two mouse cursors: one belonging to your client workstation and the other belonging to the target server. You can operate in either single mouse mode or dual mouse mode. When in dual mouse mode and properly configured, these two mouse cursors will align. If you experience difficulty with mouse synchronization, refer to Configure Target Servers.

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

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

Synchronize Mouse

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



- *To synchronize the mouse:*
 - Choose Mouse > Synchronize Mouse, or
 - Click the Synchronize Mouse button from the toolbar

Single Mouse Cursor

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

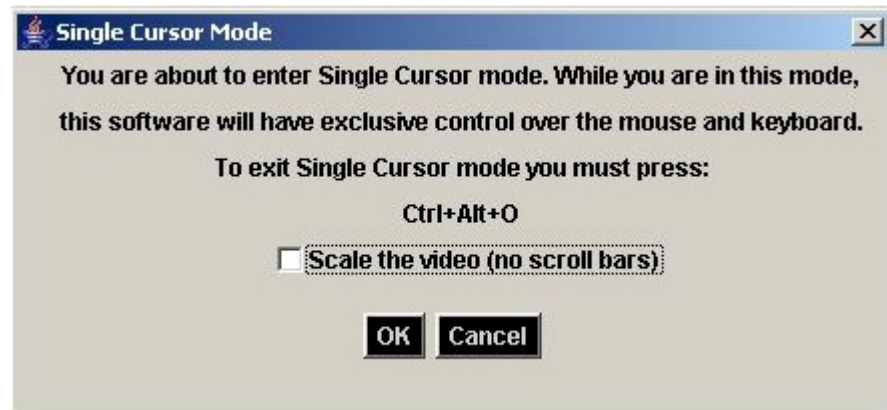


➤ *To enter single mouse mode:*

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

➤ *To exit single mouse mode:*

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



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

Standard

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

➤ *To enter standard mouse mode:*

- Choose Mouse > Standard.

Intelligent

In Intelligent mouse mode, the KX II-101 can detect the target mouse settings and synchronize the mouse pointers accordingly, allowing mouse acceleration on the target. In this mode, the mouse cursor does a “dance” in the top left corner of the screen and calculates the acceleration. For this mode to work properly, certain conditions must be met.

For additional information on Intelligent Mouse mode, refer to the Raritan Multi-Platform Client User Guide (Appendix B: Conditions for Intelligent Mouse Synchronization) available on Raritan's Website <http://www.raritan.com/support/productdocumentation>, or on the Raritan User Manuals & Quick Setup Guides CD ROM included with your KX II-101 shipment.

➤ *To enter intelligent mouse mode:*

- Choose Mouse > Intelligent.

Absolute

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

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

➤ *To enter absolute mouse mode:*

- Choose Mouse > Absolute.

Virtual Media

Refer to the chapter on **Virtual Media** (on page 102) for complete information about setting up and using virtual media.

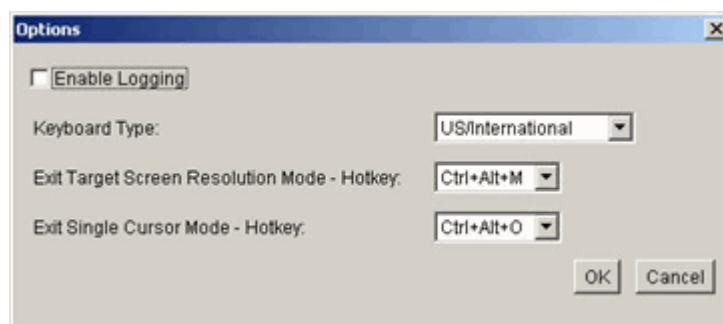
Tools Menu

Options

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

➤ *To set the tools options:*

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



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

View Menu

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

View Menu

View Toolbar

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

- *To toggle the display of the toolbar (on and off):*
 - Choose View > View Toolbar.

Scaling

Scaling your target window allows you to view the entire contents of the target server window. This feature increases or reduces the size of the target video to fit the Virtual KVM Client window size, and maintains the aspect ratio so that you see the entire target server desktop without using the scroll bar.

- *To toggle scaling (on and off):*
 - Choose View > Scaling.

Target Screen Resolution

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

- *To enter target screen resolution:*
 - Choose View > Target Screen Resolution.
- *To exit target screen resolution mode:*
 - Press the hotkey configured in the Tools Options dialog. The default is Ctrl+Alt+M.

Note to CC-SG Users: Target Screen Resolution is disabled; full screen mode is available only when the KX II-101 device is not under CC-SG management.

Help Menu

About Raritan Virtual KVM Client

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

- *To obtain version information:*
 - Choose Help > About Raritan Virtual KVM Client.

Chapter 7 Virtual Media

In This Chapter

Overview.....	103
Prerequisites for Using Virtual Media	105
Using Virtual Media	106
Opening a KVM Session	107
Connecting to Virtual Media.....	108
Disconnecting Virtual Media	111
File Server Setup (File Server ISO Images Only)	112

Overview

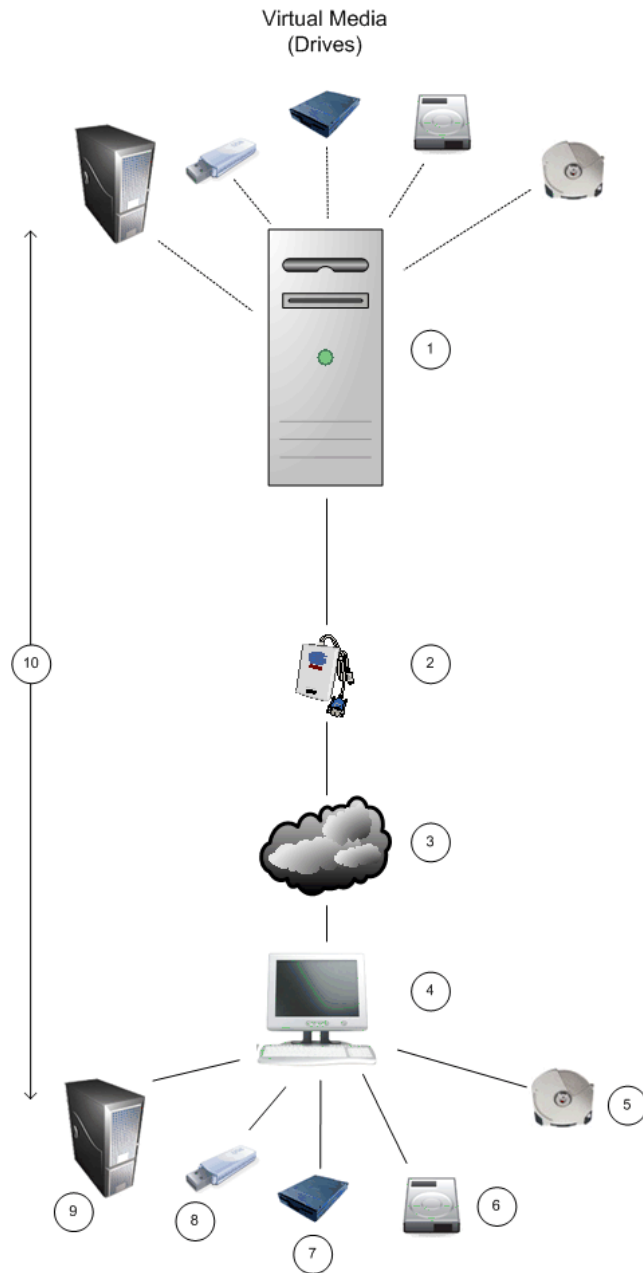
Virtual media extends KVM capabilities by enabling KVM target servers to remotely access media from the client PC and network file servers. With this feature, media mounted on the client PC and network file servers is essentially mounted virtually by the target server. The target server can then read 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.

Overview



- 1 Target server.
- 2 KX II-101
- 3 IP network connection from KX II-101 to local workstation.
- 4 Local workstation.
- 5 CD/DVD drive.
- 6 Hard drive image files.

- 7 Floppy drive.
- 8 USB drive.
- 9 Remote file server (ISO images).
- 10 Virtual connection

Prerequisites for Using Virtual Media

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

KX II-101

- For users requiring access to virtual media, KX II-101 permissions must be set to allow access to the relevant ports, as well as virtual media access (VM Access port permission) for those ports. Port permissions are set at the group-level; please refer to Setting Port Permissions for more information.
- A USB connection must exist between the KX II-101 and the target server.
- (Optional) If you want to use PC-Share, VM Share Mode must also be enabled in the Security Settings page.

Client PC

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

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

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

- USB 2.0 ports are both faster and preferred.

Target Server

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

Using Virtual Media

With the KX II-101 virtual media feature, you can mount up to two drives (of different types). These drives are accessible for the duration of the VM session.

➤ *To use virtual media:*

1. Connect/attach the media to the client or network file server that you want to access from the target server. This need not be the first step, but it must be done prior to attempting to access this media.
2. Verify that the appropriate *prerequisites* (see "Prerequisites for Using Virtual Media" on page 105) are met.
3. (File server ISO images only) If you plan to access file server ISO images, identify those file servers and images through the KX II-101 Remote Console *File Server Setup page* (see "File Server Setup (File Server ISO Images Only)" on page 112).

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

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

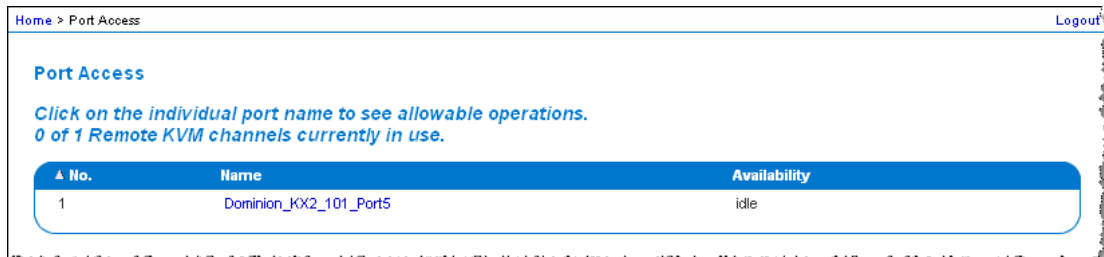
For:	Select this VM option:
Local drives	<i>Connect Drive</i> (see "Local Drives" on page 108)
Local CD/DVD drives	<i>Connect CD-ROM/ISO Image</i> (see "CD-ROM/DVD-ROM/ISO Images" on page 110)
ISO Images	Connect CD-ROM/ISO Image
File Server ISO Images	Connect CD-ROM/ISO Image

Upon completion of your tasks, *disconnect the virtual media* (see "Disconnecting Virtual Media" on page 111).

Opening a KVM Session

➤ *To open a KVM session:*

1. Open the Port Access page from the KX II-101 Remote Console.



2. Connect to the target server from the Port Access page:
 - a. Click the Name for the target server.
 - b. Select Connect from the pop-up menu.



The target server opens in a Virtual KVM Client window.

Connecting to Virtual Media

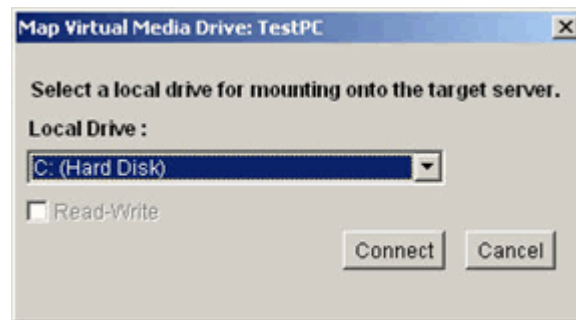
Local Drives

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

Note: KVM target servers running certain version of the Windows operating system may not accept new mass storage connections after an NTFS-formatted partition (e.g., the local C drive) has been redirected to them. If this occurs, close the KX II-101 Remote Console and reconnect before redirecting another virtual media device. If other users are connected to the same target server, they must also close their connections to the target server.

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

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



2. Choose the drive from the Local Drive drop-down list.
3. If you want read and write capabilities, select the Read-Write option checkbox. This option is disabled for non-removable drives. Please refer to the *conditions when read-write is not available* (on page 109) for more information. When checked, you will be able to read or write the connected USB disk.

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

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

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

Conditions when Read-Write is not Available

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

- For all hard drives.
- When the drive is write-protected.
- When the user does not have read-write permission:
 - Port Permission Access is set to None or View
 - Port Permission VM Access is set to Read-Only or Deny

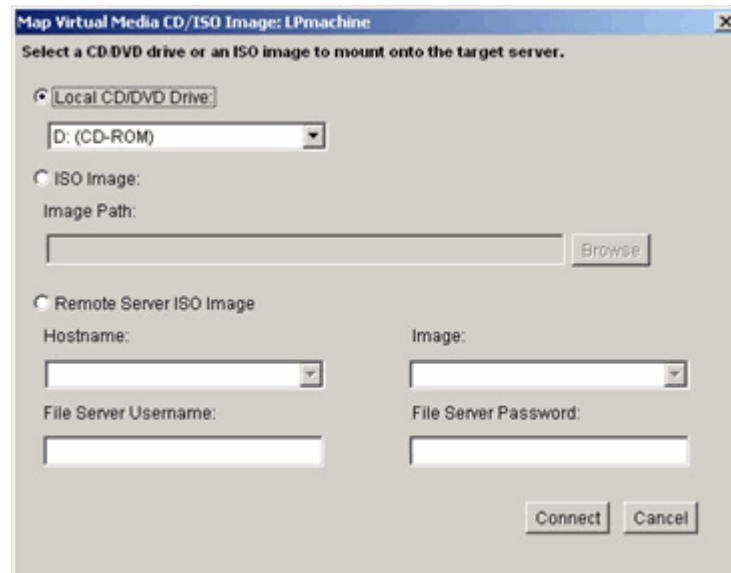
CD-ROM/DVD-ROM/ISO Images

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

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

➤ *To access a CD-ROM, DVD-ROM, or ISO image:*

1. From the Virtual KVM Client, choose Virtual Media > Connect CD-ROM/ISO Image. The Map Virtual Media CD/ISO Image dialog opens:



2. For internal and external CD-ROM or DVD-ROM drives:
 - a. Choose the Local CD/DVD Drive option.
 - b. Choose the drive from the Local CD/DVD Drive drop-down list. All available internal and external CD and DVD drive names will be populated in the drop-down list.
 - c. Click Connect.
3. For ISO images:
 - a. Choose the ISO Image option. Use this option when you want to access a disk image of a CD, DVD, or hard drive. ISO format is the only format supported.
 - b. Click the Browse button.
 - c. Navigate to the path containing the disk image you want to use and click Open. The path is populated in the Image Path field.

- d. Click Connect.
 4. For remote ISO images on a file server:
 - a. Choose the Remote Server ISO Image option.
 - b. Choose Hostname and Image from the drop-down lists. The file servers and image paths available are those that you configured using the File Server Setup page. Only items you configured using the KX II-101 File Server Setup page will be in the drop-down list.
 - c. File Server Username. Username required for access to the file server.
 - d. File Server Password. Password required for access to the file server (field is masked as you type).
 - e. Click Connect.

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

Disconnecting Virtual Media

- *To disconnect the Virtual Media drives:*
- For local drives, choose Virtual Media > Disconnect Drive.
 - For CD-ROM, DVD-ROM, and ISO images, choose Virtual Media > Disconnect CD-ROM/ISO Image.

Note: In addition to disconnecting the virtual media using the Disconnect option, simply closing the KVM connection closes the Virtual Media as well.

File Server Setup (File Server ISO Images Only)

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

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

Use the KX II-101 Remote Console File Server Setup page to designate the files server(s) and image paths that you want to access using KX II-101 Virtual Media. File server ISO image(s) specified here will become available for selection in the Remote Server ISO Image Hostname and Image drop-down lists (in the *Map Virtual Media CD/ISO Image dialog* (see "CD-ROM/DVD-ROM/ISO Images" on page 110)).

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

1. Choose Virtual Media from the KX II-101 Remote Console. The File Server Setup page opens:

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

Save Cancel

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

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

Chapter 8 Device Management

In This Chapter

Device Settings Menu.....	114
Network Settings	115
Device Services.....	120
Keyboard/Mouse Settings.....	122
Serial Port Settings.....	123
Date/Time Settings.....	124
Event Management.....	125
Port Configuration.....	131

Device Settings Menu

The Device Settings menu is organized as follows: Network, Device Services, Keyboard/Mouse, Serial Port, Date/Time, Event Management - Settings, Event Management - Destinations, and Port Configuration.

Use:	To:
Network	Customize the network configuration for the KX II-101.
Device Services	Configure KX II-101 network port and enable TELNET and SSH access.
Keyboard/Mouse	Configure how the target server sees the keyboard and mouse signals KX II-101 sends.
Serial Port	Select and configure the function of KX II-101's serial port.
Date/Time	Set date, time, time zone, and Network Time Protocol (NTP).
Event Management - Settings	Configure SNMP and Syslog.
Event Management - Destinations	Select which system events to track and where to send this information.
Port Configuration	Configure KVM ports, and outlets.

Network Settings

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

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

- None. (Default) This option 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. 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.

Home > Device Settings > Network Settings

Network Basic Settings

Device Name *

DKX2-101

IP auto configuration

DHCP

Preferred host name (DHCP only)

IP address

192.168.50.74

Subnet mask

255.255.255.0

Gateway IP address

192.168.50.126

Primary DNS server IP address

192.168.50.114

Secondary DNS server IP address

192.168.50.112

OK Reset To Defaults Cancel

LAN Interface Settings

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.

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

LAN Interface Speed & Duplex

Autodetect

Bandwidth Limit

No Limit

Set System ACL

2. Update the Network Basic Settings. Refer to Network Basic Settings for more information about each of the fields.
3. Update the LAN Interface Settings. Refer to LAN Interface Settings for more information about each of the fields.
4. Click OK to set these configurations. If your changes require rebooting the device, a reboot message appears.

Network Settings

➤ *To cancel without saving changes:*

- Click Cancel.

➤ *To reset to factory defaults:*

- Click Reset to Defaults.

Network Basic Settings

Network Basic Settings

Device Name *
DKX2-101

IP auto configuration
DHCP ▼

Preferred host name (DHCP only)

IP address
192.168.59.99

Subnet mask
255.255.255.0

Gateway IP address
192.168.59.126

Primary DNS server IP address
192.168.59.2

Secondary DNS server IP address
192.168.51.10

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

- **Device Name.** Type a unique name for the device (up to 16 characters; spaces are not allowed). Name your device so you can easily identify it. The default name for a KX II-101 unit is: “DKX2-101”. Remote users will also see this name. However, if an MPC user has created a Connection Profile for this device, that user will see the Description field from the Profile instead.
- **IP auto configuration.** Select from among the options available in the drop-down list:
 - **None.** Use this option if you do not want an auto IP configuration and prefer to set the IP Address yourself (static IP). This is the default and recommended option.

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

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

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

LAN Interface Settings

LAN Interface Settings

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.

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

LAN Interface Speed & Duplex
Autodetect

Bandwidth Limit
No Limit

[Set System ACL](#)

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

Autodetect	Default option	
10 Mbps/Half		Both LEDs blink
10 Mbps/Full		Both LEDs blink
100 Mbps/Half		Yellow LED blinks
100 Mbps/Full		Yellow LED blinks
1000 Mbps/Full	Gigabit	Green LED blinks

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

Full-duplex allows communication in both directions simultaneously.

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

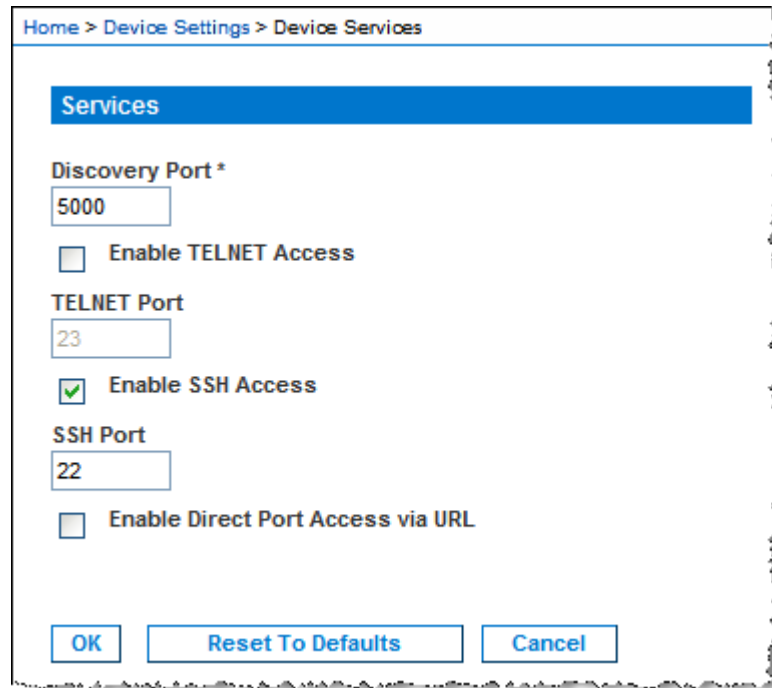
Please refer to Network Speed Settings for more information.

- Bandwidth Limit. Select among the bandwidth limits available.
 - 128 Kilobit
 - 256 Kilobit
 - 512 Kilobit
 - 2 Megabit
 - 5 Megabit
 - 10 Megabit
 - 100 Megabit
 - No Limit
- Set System ACL. Click this button to set a global-level Access Control List for your KX II-101 by ensuring that your device does not respond to packets being sent from disallowed IP addresses. The *IP Access Control* (on page 151) page opens.

Note: These ACL values are global, affecting the KX II-101 unit as a whole. You can also create ACLs on a group-level basis. For example, you can create an “Outsourced Vendors” user group that is permitted to access KX II-101 only from a given IP address range (refer to Group-based IP ACL for more information on how to create group-specific Access Control Lists).

Device Services

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



The screenshot shows a web interface for configuring device services. At the top, a breadcrumb trail reads "Home > Device Settings > Device Services". Below this is a blue header bar labeled "Services". The configuration options are as follows:

- Discovery Port ***: A text input field containing the value "5000".
- Enable TELNET Access**: An unchecked checkbox.
- TELNET Port**: A text input field containing the value "23".
- Enable SSH Access**: A checked checkbox.
- SSH Port**: A text input field containing the value "22".
- Enable Direct Port Access via URL**: An unchecked checkbox.

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

➤ *To configure the discovery port:*

1. Choose Device Settings > Device Services. The Device Services page opens.
2. Type the network port used by 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 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.
2. Select Enable SSH Access.
3. Type the network port used for SSH access to 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 an 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 an URL with the IP address, user name, password, and if necessary, port number of the KX II-101. If you have only one KVM port, the port number is not needed.

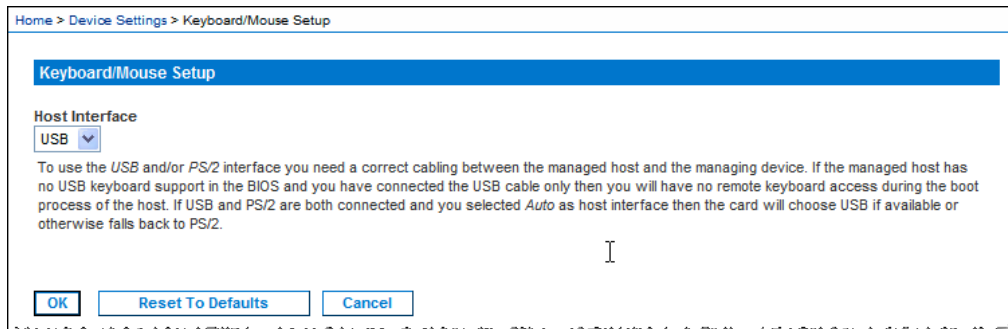
The format for a direct port access URL is:

`https://[IP
address]/dpa.asp?username=[username]&password=[password]&po
rt=[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 Settings

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



- Host Interface. Selects whether the KX II-101 sends keyboard and mouse data through the PS/2 or USB connections.
 - Auto. With this setting, KX II-101 will use a USB connection if available and fall back on the PS/2 connection if not.
 - USB. Forces KX II-101 to use the USB connection to send Keyboard and Mouse data to the host device.
 - PS/2. Forces KX II-101 to use the PS/2 connection to send Keyboard and Mouse data to the host device.
- *To reset to factory defaults*
- Click Reset To Defaults.

Serial Port Settings

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

➤ *To configure the serial port:*

1. Choose Device Settings > Serial Port. The Serial Port Settings page opens:

The screenshot shows a 'Serial Port Settings' window. It has three radio buttons: 'Admin Port' (selected), 'Powerstrip Control', and 'Modem'. Below these, under the heading 'Serial Settings:', there are five dropdown menus: 'Speed' (set to 115200), 'Stop Bits' (set to 1), 'Data bits' (set to 8), 'Handshake' (set to None), and 'Parity' (set to none). At the bottom of the window are three buttons: 'OK', 'Reset To Defaults', and 'Cancel'.

2. Choose the function you would like for the serial port:
 - Admin Port. Choose this option to connect to the KX II-101 directly from a client PC order to access advanced configuration.
 - PowerStrip Control. Chose this option when connecting the KX II-101 to a serially controlled power strip.
 - Modem. Choose this option when attaching an external modem to the KX II-101 in order to provide dial-in access.
3. For the Modem option, enter configure the modem use settings as follows:
 - a. Select the data speed between KX II-101 and the modem from the Serial line speed drop-down list.
 - b. Enter the Modem init string.
 - c. Enter a Modem server IP address. This will be the address the user types to access the KX II-101 web interface once they have connected via modem.
 - d. Enter a Modem client IP address. This will be the address assigned to the user once they have connected via modem.
4. Click OK.

Date/Time Settings

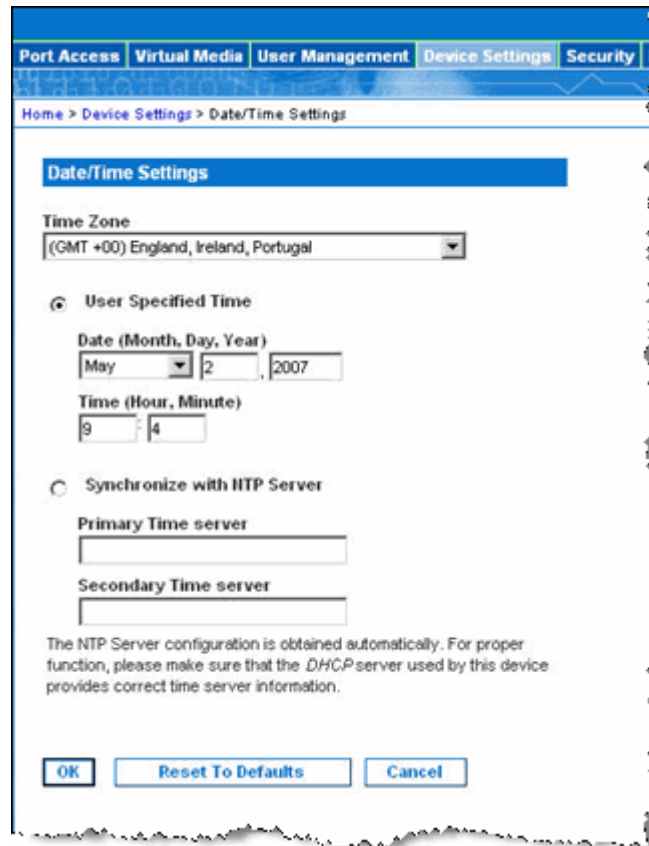
Use the Date/Time Settings page to specify the date and time for the KX II-101. There are two ways to do this:

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

Note: The KX II-101 does not support Daylight Savings Time.

➤ *To set the date and time:*

1. Choose Device Settings > Date/Time. The Date/Time Settings page opens:



The screenshot shows the 'Date/Time Settings' page within a web interface. At the top, there is a navigation bar with tabs: 'Port Access', 'Virtual Media', 'User Management', 'Device Settings' (which is active), and 'Security'. Below the navigation bar, a breadcrumb trail reads 'Home > Device Settings > Date/Time Settings'. The main content area is titled 'Date/Time Settings' and contains the following elements:

- A 'Time Zone' dropdown menu currently set to '(GMT +00) England, Ireland, Portugal'.
- Two radio buttons for selecting the time setting method:
 - ☒ 'User Specified Time': This option is selected. It includes a 'Date (Month, Day, Year)' section with a month dropdown (set to 'May'), a day input field (set to '2'), and a year input field (set to '2007'). Below this is a 'Time (Hour, Minute)' section with an hour input field (set to '9') and a minute input field (set to '4').
 - ☐ 'Synchronize with NTP Server': This option is unselected. It includes two text input fields labeled 'Primary Time server' and 'Secondary Time server'.
- A note at the bottom: 'The NTP Server configuration is obtained automatically. For proper function, please make sure that the DHCP server used by this device provides correct time server information.'
- At the bottom of the form are three buttons: 'OK', 'Reset To Defaults', and 'Cancel'.

2. Choose your time zone from the Time Zone drop-down list.
3. Choose the method you would like to use to set the date and time:
 - User Specified Time. Choose this option to input the date and time manually.

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

Event Management

The 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.

SNMP Configuration

Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions. KX II-101 offers SNMP Agent support through Event Management. Refer to *SNMP Agent Configuration* (on page 129) and *SNMP Trap Configuration* (on page 129) for more information about SNMP Agents and Traps.

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

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

Home > Device Settings > Event Management - Settings

SNMP Configuration

☐ SNMP Logging Enabled

Name
sai-Dlx2101

Contact
SAI

Location
FSD

Agent Community String

Type
Read-Write

Destination IP	Port #	Community
192.168.51.150	162	public
	162	public
	162	public
	162	public
	162	public

[Click here to view the Dominion KX2-101 SNMP MIB](#)

SysLog Configuration

☐ Enable Syslog Forwarding

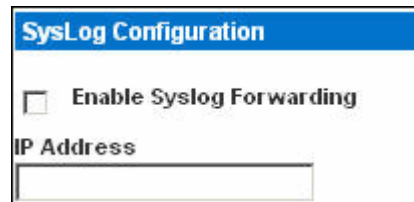
IP Address

OK Reset To Defaults Cancel

2. Select the Enable SNMP Logging option; this enables the remaining SNMP fields.
3. In the Name, Contact, and Location fields, type the SNMP Agent's (this Dominion unit's) name as it appears in the KX II-101 Console interface, a contact name related to this unit, and where the Dominion unit is physically located, respectively.

4. Type the Agent Community String (the Dominion unit's string). An SNMP community is the group that devices and management stations running SNMP belong to; it helps define where information is sent. The community name is used to identify the group; an SNMP device or agent may belong to more than one SNMP community.
5. Specify whether the community is Read-Only or Read-Write using the Type drop-down list.
6. Configure up to five SNMP managers by specifying their Destination IP, Port #, and Community.
7. Click the Click here to view the KX II-101 SNMP MIB link to access the SNMP Management Information Base.
8. Click OK.

Syslog Configuration



The image shows a 'SysLog Configuration' dialog box. It has a blue title bar with the text 'SysLog Configuration'. Below the title bar, there is a checkbox labeled 'Enable Syslog Forwarding'. Underneath the checkbox, there is a label 'IP Address' followed by a text input field.

- *To configure the Syslog (enable Syslog forwarding):*
 1. Choose the Enable Syslog Forwarding option to log the device's messages to a remote Syslog server.
 2. Type the IP Address of your Syslog server in the IP Address field.
 3. Click OK.
- *To cancel without saving changes:*
 - Click Cancel.
- *To reset to factory defaults:*
 - Click the Reset To Defaults button.

Event Management - Destinations

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

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

➤ *To select events and their destinations:*

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

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	System Startup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Power Supply Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Powerstrip Outlet Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Parameter Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Ethernet Failover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Management	Factory/Reset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Begin OC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	End OC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Started	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Completed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware Update Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware File Discarded	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware Validation Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Configuration Backed Up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Configuration Restored	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Connection Denied	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security	Password Settings Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Login Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Password Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Activity	User Blocked	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Connected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Disconnected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

2. Select the checkboxes for those Event line items you want to enable or disable, and where you want to send the information.

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

3. Click OK.

➤ *To cancel without saving changes:*

- Click Cancel.

➤ *To reset to factory defaults:*

- Click the Reset To Defaults button.

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

SNMP Agent Configuration

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

SNMP Trap Configuration

SNMP provides the ability to send traps, or notifications, to advise an administrator when one or more conditions have been met. The following table lists the KX II-101 SNMP traps:

Trap Name	Description
configBackup	The device configuration has been backed up.
configRestore	The device configuration has been restored.
deviceUpdateFailed	Device update has failed.
deviceUpgradeCompleted	The KX II-101 has completed update via an RFP file.
deviceUpgradeStarted	The KX II-101 has begun update via an RFP file.
factoryReset	The device has been reset to factory defaults.

Trap Name	Description
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.
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.

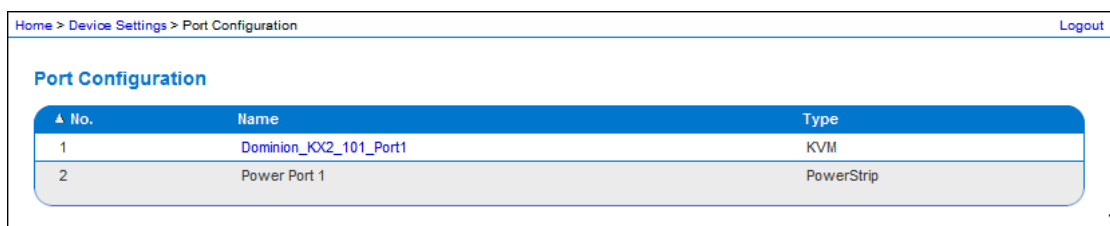
Trap Name	Description
userAuthenticationFailure	A user attempted to log in without a correct username and/or password.
userConnectionLost	A user with an active session has experienced an abnormal session termination.
userDeleted	A user account has been deleted.
userLogin	A user has successfully logged into the KX II-101 and has been authenticated.
userLogout	A user has successfully logged out of the KX II-101 properly.
userModified	A user account has been modified.
userPasswordChanged	This event is triggered if the password of any user of the device is modified.
userSessionTimeout	A user with an active session has experienced a session termination due to timeout.
vmImageConnected	User attempted to mount either a device or image on the target using Virtual Media. For every attempt on device/image mapping (mounting) this event is generated.
vmImageDisconnected	User attempted to unmount a device or image on the target using Virtual Media.

Port Configuration

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

➤ *To change a port configuration:*

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



Port Configuration

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 unit.
- Port Name. The name assigned to the port. A port name displayed in black indicates that you cannot change the name and that the port cannot be edited; port names displayed in blue can be edited.

Note: Do not use apostrophes for the Port Name.

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

Port Type	Description
PowerStrip	Powerstrip
KVM	KVM Target

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

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

Chapter 9 Power Control

In This Chapter

Overview.....	133
Connect the Power Strip	133
Name the Power Strip (Port Page for Power Strips).....	135
Associate KVM Target Servers to Outlets (Port Page).....	136
Displaying the Outlet Associations.....	140
Control the Powerstrip Device.....	141

Overview

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:*

1. Connect the power strip to your target server.
2. Name the power strip.
3. Associate outlet in the power strip to the target server.
4. Turn the outlets on the powerstrip on and off in the **Powerstrip Device** (see "Control the Powerstrip Device" on page 141) page.

Connect the Power Strip



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

Connect the Power Strip

2 Raritan power strip.

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

1. Connect the Mini DIM9M 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.

Name the Power Strip (Port Page for Power Strips)

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

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

Home > Device Settings > Port Configuration > Port

Port 1

Type:
KVM

Name:

Power Association

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

Target Server Settings

☐ Use Full Speed - Useful for BIOS that cannot handle High Speed USB devices

☐ Absolute mouse scaling for MAC server (applies only if USB is active Keyboard/Mouse Interface)

☐ USB SUN Keyboard support (applies only if USB is active Keyboard/Mouse Interface)

OK Cancel

Associate KVM Target Servers to Outlets (Port Page)

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 #.)
3. Click OK.

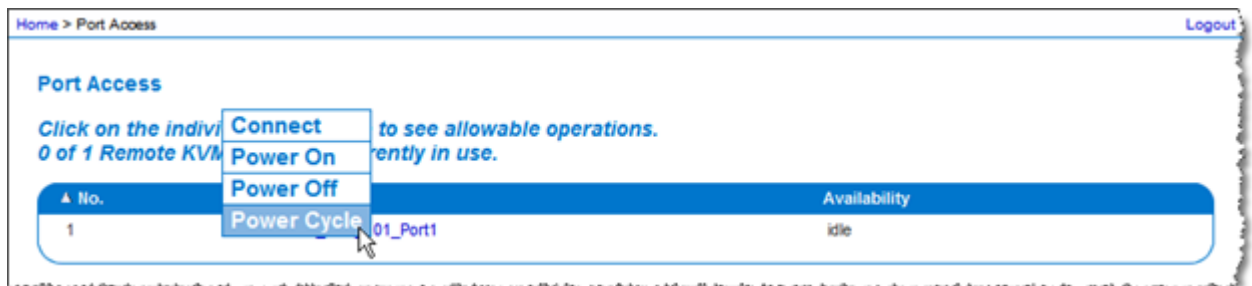
➤ *To cancel without saving changes:*

- Click Cancel.

Associate KVM Target Servers to Outlets (Port Page)

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

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



Note: To use this feature, you must have a Raritan Dominion PX power strip attached to the device. See *Connect the Power Strip* (on page 133) for information.

- *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 is displayed.

Associate KVM Target Servers to Outlets (Port Page)

A powerstrip with two outlet associations is shown below.

The screenshot shows a web-based configuration interface for a KVM port. The breadcrumb navigation at the top reads: Home > Device Settings > Port Configuration > Port. The main section is titled "Port 1" in a blue header. Below this, the "Type" is set to "KVM" and the "Name" is "Dominion_KX2_101_Port1". The "Power Association" section contains a "Power Strip Name" dropdown set to "Power Port 1" and two "Outlet Name" dropdowns, both set to "Dominion_KX2_101_Port1(7)" and "Dominion_KX2_101_Port1(8)" respectively. The "Target Server Settings" section has three unchecked checkboxes: "Use Full Speed - Useful for BIOS that cannot handle High Speed USB devices", "Absolute mouse scaling for MAC server (applies only if USB is active Keyboard/Mouse Interface)", and "USB SUN Keyboard support (applies only if USB is active Keyboard/Mouse Interface)". At the bottom are "OK" and "Cancel" buttons.

Home > Device Settings > Port Configuration > Port

Port 1

Type:
KVM

Name:
Dominion_KX2_101_Port1

Power Association

Power Strip Name: Power Port 1

Outlet Name:
Dominion_KX2_101_Port1(7)
Dominion_KX2_101_Port1(8)
None
None

Target Server Settings

☐ Use Full Speed - Useful for BIOS that cannot handle High Speed USB devices

☐ Absolute mouse scaling for MAC server (applies only if USB is active Keyboard/Mouse Interface)

☐ USB SUN Keyboard support (applies only if USB is active Keyboard/Mouse Interface)

OK Cancel

➤ *To change the port name:*

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

- *To cancel without saving changes:*
 - Click Cancel.

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

Displaying the Outlet Associations

- *To show the power port configuration:*
- Choose Home > Device Settings > Port Configuration > [power port name].

The outlet associations for the powerstrip appear under Outlets.

The screenshot shows a web-based configuration interface for a power strip. At the top, a breadcrumb trail reads 'Home > Device Settings > Port Configuration > Port'. Below this, a blue header bar identifies the section as 'Port 2'. The 'Type' is set to 'PowerStrip'. The 'Name' field contains 'Power Port 1'. A section titled 'Outlets' contains a table with 8 rows. The first six rows are labeled 'Outlet 1' through 'Outlet 6' and have no associations. The last two rows, 'Outlet 7' and 'Outlet 8', both have the name 'Dominion_KX2_101_Port1' and are associated with 'Dominion_KX2_101_Port1'. At the bottom are 'OK' and 'Cancel' buttons.

Number	Name	Port Association
1	Outlet 1	
2	Outlet 2	
3	Outlet 3	
4	Outlet 4	
5	Outlet 5	
6	Outlet 6	
7	Dominion_KX2_101_Port1	Dominion_KX2_101_Port1
8	Dominion_KX2_101_Port1	Dominion_KX2_101_Port1

- *To edit the power port configuration:*
 - Change the Powerport name by editing the Port 2 > Name field.
 - Change an outlet name by editing the associated Outlets > Name field. The outlet name appears in the Powerstrip Device page. See *Control the Powerstrip Device* (on page 141) for information.
 - Change the outlet association by clicking the Port Association link next to the outlet name and editing it in the Port 1 page. See *Associate KVM Target Servers to Outlets (Port Page)* (on page 136) for information.

Control the Powerstrip Device

You can control the powerstrip device using the Powerstrip Device page. This page enables you to turn each outlet on the powerstrip on and off.

Home > Powerstrip

Powerstrip Device

Powerstrip: Power Port 1 - PCR8 Update

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

Outlet 1

off

1

On Off

Outlet 2

off

2

On Off

Outlet 3

off

3

On Off

Outlet 4

off

4

On Off

Outlet 5

off

5

On Off

Outlet 6

off

6

On Off

Outlet 7

on

7

On Off

Outlet 8

on

8

On Off

- *To control the powerstrip connected to the KX II-101:*
 1. Choose Home > Powerstrip.

Control the Powerstrip Device

The Powerstrip 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.

The power outlet is powered on or off.

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

Chapter 10 Security Settings

In This Chapter

Security Settings Menu	143
Security Settings.....	144
IP Access Control.....	151

Security Settings Menu

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

Use:	To:
Security Settings	Configure security settings for login limitations, strong passwords, user blocking, and encryption & share.
IP Access Control	Control access to your KX II-101 unit. By setting a global access control list, you are by ensuring that your device does not respond to packets being sent from disallowed IP addresses.

Security Settings

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

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

➤ *To configure the security settings:*

1. Choose Security > Security Settings. The Security Settings page opens.

The screenshot shows the 'Security Settings' page with the following configuration:

- Login limitations:**
 - ☐ Enable Single Login Limitation
 - ☐ Enable Password Aging
 - Password Aging Interval (days): 60
 - ☐ Log Out Idle Users
 - After (minutes): 30
- User Blocking:**
 - ☒ Disabled
 - ☐ Timer Lockout
 - Attempts: 3
 - Lockout Time: 5
 - ☐ Deactivate User-ID
 - Failed Attempts: 3
- Strong passwords:**
 - ☐ Enable strong passwords
 - Minimum length of strong password: 8
 - Maximum length of strong password: 16
 - ☒ Enforce at least one lower case character
 - ☒ Enforce at least one upper case character
 - ☒ Enforce at least one numeric character
 - ☒ Enforce at least one printable special character
 - Number of restricted passwords based on history: 5
- Encryption & Share:**
 - Encryption Mode: Auto
 - ☒ Apply Encryption Mode to KVM and Virtual Media
 - PC Share Mode: PC-Share
 - ☐ VM Share Mode
 - ☐ Disable Local Port Output
 - Local Device Reset Mode: Enable Local Factory Reset

Buttons at the bottom: OK, Reset To Defaults, Cancel.

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

2. Update the **Login Limitations** (on page 145) settings as appropriate.
3. Update the **Strong Passwords** (on page 146) settings as appropriate.
4. Update the **User Blocking** (on page 147) settings as appropriate.
5. Update the Encryption & Share settings as appropriate.
6. Click OK.

➤ *To close the page without saving any changes:*

- Click Cancel.

➤ *To reset back to defaults:*

- Click Reset to Defaults.

Login Limitations

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

- **Enable Single Login Limitation.** When selected only one login per username is allowed at any time. When deselected, a given username/password combination can be connected into the device from several client workstations simultaneously.
- **Enable Password Aging.** When selected all users are required to change their passwords periodically, based on the number of days specified in Password Aging Interval field.
 - **Password Aging Interval (days).** This field is enabled and required when the Enable Password Aging checkbox is selected. Enter the number of days after which a password change is required. The default is 60 days.
- **Log Out Idle Users.** Select the checkbox to automatically disconnect a user session after a certain amount of inactive time has passed. Type the amount of time in the After field. If there is no activity from the keyboard or mouse, all sessions and all resources are logged out. If a Virtual Media session is in progress, however, the session does not timeout.
 - **After (minutes).** The amount of time (in minutes) after which an idle user will be logged out. This field is enabled when the Log Out Idle Users option is selected.

Strong Passwords

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

- Enable strong passwords. Strong passwords require user-created passwords to have a minimum of 8 characters with at least one alphabetical character and one non-alphabetical character (punctuation character or number). In addition, the first four characters of the password and the username cannot match. When selected, strong password rules are enforced. Users with passwords not meeting strong password criteria will automatically be required to change their password on their next login. When deselected, only the standard format validation is enforced. When selected, the following fields are enabled and required:
 - Minimum length of strong password. Passwords must be at least 8 characters long. The default is 8, but it can be up to 63.
 - Maximum length of strong password. The default is 16, but can be up to 64 characters long.
 - Enforce at least one lower case character. When checked, at least one lower case character is required in the password.
 - Enforce at least one upper case character. When checked, at least one upper case character is required in the password.
 - Enforce at least one numeric character. When checked, at least one numeric character is required in the password.

- Enforce at least one printable special character. When checked, at least one special character (printable) is required in the password.
- Number of restricted passwords based on history. This field represents the password history depth; that is, the number of prior passwords that cannot be repeated. The range is 1-12; the default is 5.

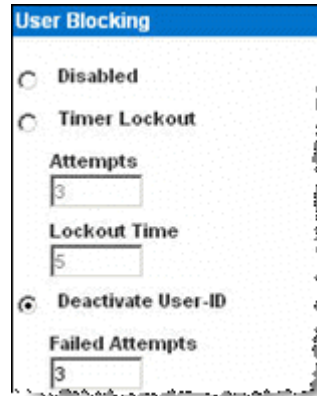
User Blocking

The User Blocking options specify the criteria by which users are blocked from accessing the system after the specified number of unsuccessful login attempts. The three options are mutually exclusive:

- Disabled. The default option; users are not blocked regardless of the number of times they fail authentication.
- Timer Lockout. Users are denied access to the system for the specified amount of time after exceeding the specified number of unsuccessful login attempts. When selected, the following fields are enabled:
 - Attempts. The number of unsuccessful login attempts after which the user will be locked out. The valid range is 1 - 10; the default is 3 attempts.
 - Lockout Time. The amount of time for which the user will be locked out. The valid range is 1 - 1440 minutes; the default is 5 minutes.

Security Settings

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

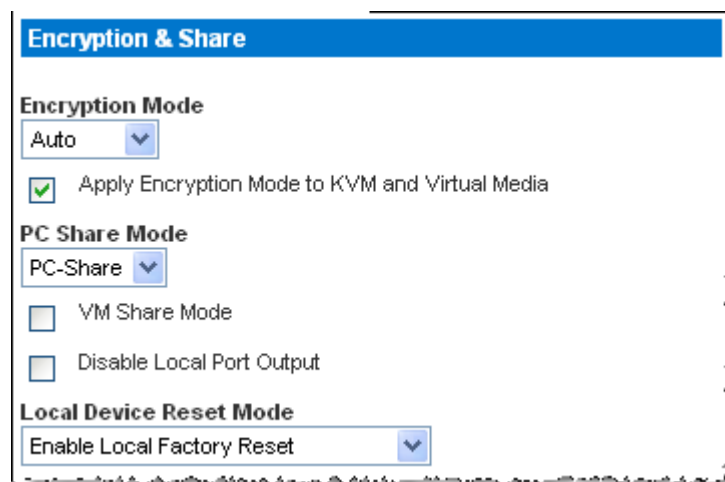


The screenshot shows a window titled "User Blocking". It contains three radio button options: "Disabled", "Timer Lockout", and "Deactivate User-ID". The "Deactivate User-ID" option is selected. Below the radio buttons, there are two input fields: "Attempts" with the value "3" and "Lockout Time" with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

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* (see "Add New User" on page 50) page.

Encryption and Share

Using the Encryption & Share settings you can specify the type of encryption used, PC and VM share modes, and the type of reset performed when the KX II-101 reset button is pressed.



The screenshot shows a window titled "Encryption & Share". It contains three sections: "Encryption Mode" with a dropdown menu set to "Auto" and a checked checkbox "Apply Encryption Mode to KVM and Virtual Media"; "PC Share Mode" with a dropdown menu set to "PC-Share" and two unchecked checkboxes "VM Share Mode" and "Disable Local Port Output"; and "Local Device Reset Mode" with a dropdown menu set to "Enable Local Factory Reset".

- Encryption Mode. Choose one of the options from the drop-down list. When an encryption mode is selected, a warning is displayed that if your browser does not support the selected mode, you will not be able to connect to the KX II-101:

Encryption & Share

When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the Dominion KX2-101.

Encryption Mode

RC4 ▼

☒ Apply Encryption Mode to KVM and Virtual Media

PC Share Mode

Private ▼

☐ VM Share Mode

☐ Disable Local Port Output

Local Device Reset Mode

Enable Local Factory Reset ▼

- Auto. This is the recommended option; the KX II-101 auto-negotiates to the highest level of encryption possible.
- RC4. Secures user names, passwords and KVM data, including video transmissions using the RSA RC4 encryption method. This is a 128-bit Secure Sockets Layer (SSL) protocol which provides a private communications channel between the KX II-101 unit and the Remote PC during initial connection authentication.
- AES-128. The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data; 128 is the key length. When AES-128 is specified, please be certain that your browser supports it, otherwise you will not be able to connect. Please refer to *Checking Your Browser for AES Encryption* (on page 151) for more information.
- AES-256. The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data; 256 is the key length. When AES-256 is specified, please be certain that your browser supports it, otherwise you will not be able to connect. Please refer to *Checking Your Browser for AES Encryption* (on page 151) for more information.

Security Settings

- 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.
- PC Share Mode. Determines global concurrent remote KVM access, enabling up to eight remote users to simultaneously log on to one KX II-101 and concurrently view and control the same target server through the device. Click on the drop-down list to select one of the following options:
 - Private: No PC share; this is the default mode. Each target server can be accessed exclusively by only one user at a time.
 - PC-Share: KVM target servers can be accessed by up to eight users (administrator or non-administrator) at one time. Each remote user has equal keyboard and mouse control, however, please note that uneven control will occur if one user does not stop typing or moving the mouse.
- VM Share Mode. This option is enabled only when PC-Share Mode is enabled. When selected, this option permits the sharing of virtual media among multiple users, that is, several users can access the same virtual media session. The default is disabled.
- Local Device Reset Mode. This option specifies which actions are taken when the hardware reset button (at the back of the unit) is depressed. For more information, refer to Reset Button. Select one of the following options:
 - Enable Local Factory Reset (Default). Returns the KX II-101 unit to the factory defaults.
 - Enable Local Admin Password Reset. Resets the local administrator password only. The password is reset to raritan.
 - Disable All Local Resets. No reset action is taken.

Checking Your Browser for AES Encryption

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

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

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

AES 256 Prerequisites and Supported Configurations

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

- Firefox 2.0.0.7
- Mozilla 1.7.13
- Internet Explorer 7

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

Jurisdiction files for various JRE's are available at the "other downloads" section of the following links:

- JRE1.4.2 - <http://java.sun.com/j2se/1.4.2/download.html>
- JRE1.5 - http://java.sun.com/javase/downloads/index_jdk5.jsp

IP Access Control

Using IP Access Control, you can control access to your KX II-101 unit. By setting a global Access Control List (ACL) you are by ensuring that your device does not respond to packets being sent from disallowed IP addresses. The IP Access Control is global, affecting the KX II-101 unit as a whole, but you can also control access to your unit at the group level. Refer to group-based IP Access Control for more information about group-level control.

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 using one of these methods:

IP Access Control

- Choose Security > IP Access Control, or
- Click the Set System ACL button from the Network Settings page

The IP Access Control page opens:

Port Access Virtual Media User Management Device Settings Security Maintenance

Home > Security > IP Access Control

IP Access Control

☐ Enable IP Access Control

Default policy
ACCEPT

Rule #	IP/Mask	Policy
		ACCEPT

Append Insert Replace Delete

Apply Reset To Defaults Cancel

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.
2. Choose the Policy from the drop-down list.
3. Click Append. The rule is added to the bottom of the rules list.
4. Repeat steps 1 through 3 for each rule you want to enter.

➤ *To insert a rule:*

1. Type a Rule #. A Rule # is required when using the Insert command.
2. Type the IP Address and subnet mask in the IP/Mask field.
3. Choose the Policy from the drop-down list.

4. Click Insert. If the Rule # you just typed equals an existing Rule #, the new rule is placed ahead of the exiting rule and all rules are moved down in the list.

➤ *To replace a rule:*

1. Specify the Rule # you want to replace.
2. Type the IP Address and subnet mask in the IP/Mask field.
3. Choose the Policy from the drop-down list.
4. Click Replace. Your new rule replaces the original rule with the same Rule #.

➤ *To delete a rule:*

1. Specify the Rule # you want to delete.
2. Click Delete.
3. You are prompted to confirm the deletion. Click OK.

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

Chapter 11 Maintenance

In This Chapter

Maintenance Menu	154
Audit Log.....	155
Device Information.....	156
Backup and Restore	157
Firmware Upgrade	159
Upgrade History	161
Reboot.....	161

Maintenance Menu

The Maintenance menu includes these options: Audit Log, Device Information, Backup/Restore, Firmware Upgrade, Factory Reset, Upgrade History, and Reboot.

Audit Log

A log is created of KX II-101 system events.

➤ *To view the audit log for your KX II-101 unit:*

1. Choose Maintenance > Audit Log. The Audit Log page opens:

Date	Event	Description
11/13/2007 12:51:53	Access Logout	User 'admin' from host '192.168.61.209' logged out.
11/13/2007 12:28:01	Port Status Changed	Status of port 'Dominion_KX2_101_Port5' changed to 'available'.
11/13/2007 12:28:01	Port Disconnected	Port 'Dominion_KX2_101_Port5' disconnected by user 'admin'.
11/13/2007 12:27:56	Port Status Changed	Status of port 'Dominion_KX2_101_Port5' changed to 'connected'.
11/13/2007 12:27:56	Port Connected	Port 'Dominion_KX2_101_Port5' connected by user 'admin'.
11/13/2007 11:39:00	Access Login	User 'admin' from host '192.168.61.209' logged in.
11/13/2007 10:55:30	Access Login	User 'admin' from host '192.168.50.54' logged in.
11/13/2007 10:55:15	Login Failed	Authentication failed for user 'admin' from host '192.168.50.54'.
11/12/2007 17:53:55	Access Logout	User 'admin' from host '192.168.32.40' logged out.
11/12/2007 17:53:28	Access Login	User 'admin' from host '192.168.32.40' logged in.
11/12/2007 17:53:13	Access Logout	User 'CC admin' from host '192.168.59.246' logged out.
11/12/2007 17:53:13	End CC Control	CC management stopped by user 'CC admin' from host '192.168.59.246'.
11/12/2007 17:50:19	Access Logout	User 'CC user session' from host '192.168.59.246' logged out.
11/12/2007 17:48:21	Access Login	User 'CC user session' from host '192.168.59.246' logged in.
11/12/2007 17:48:16	Access Logout	User 'CC admin' from host '192.168.59.246' logged out.
11/12/2007 17:48:15	Access Login	User 'CC admin' from host '192.168.59.246' logged in.
11/12/2007 17:48:14	Access Login	User 'CC admin' from host '192.168.59.246' logged in.
11/12/2007 17:48:08	Access Logout	User 'admin' from host '192.168.59.246' logged out.
11/12/2007 17:48:08	Begin CC Control	CC management started by user 'admin' from host '192.168.59.246'.
11/12/2007 17:48:08	Access Logout	User 'admin' from host '192.168.59.246' logged out.

The Audit Log page displays events by date and time (most recent events listed first). The Audit Log provides the following information:

- **Date.** The date and time that the event occurred; 24-hour clock.
- **Event.** The event name as listed in the Event Management page.
- **Description.** Detailed description of the event.

➤ *To save the Audit Log:*

Note: Saving the Audit Log is available only on the KX II-101 Remote Console, not on the Local Console.

1. Click the Save to File button. A Save File dialog opens.

Device Information

2. Select 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:*

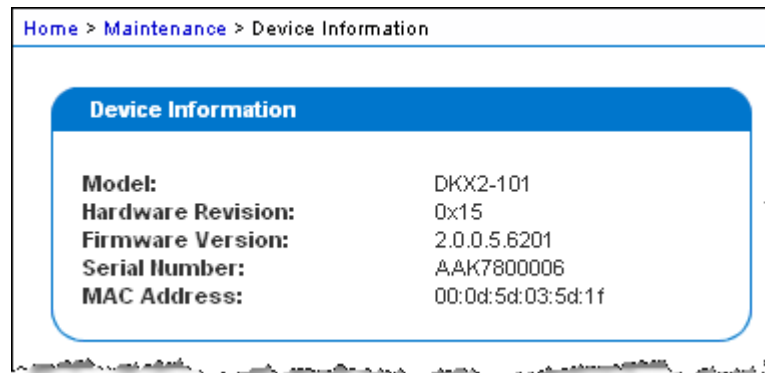
- Use the [Older] and [Newer] links.

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:



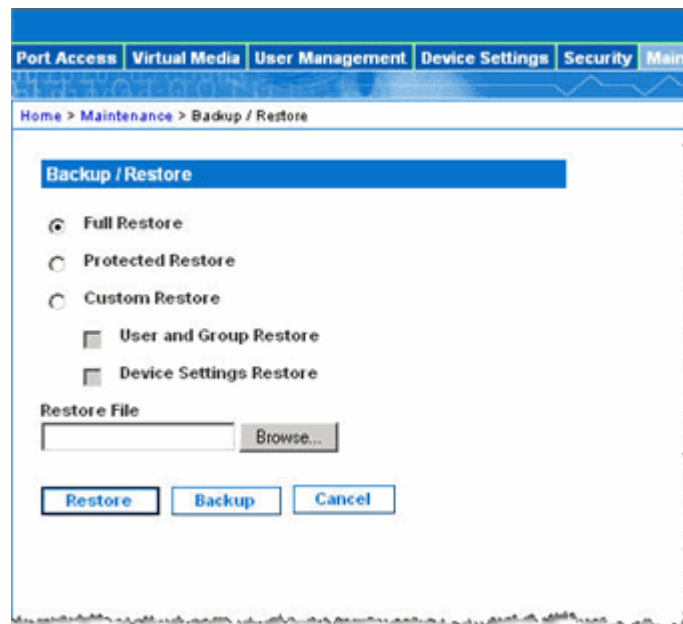
The following information is provided about the KX II-101: Model, Hardware Revision, Firmware Version, Serial Number, and MAC Address.

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 setup one KX II-101 and copy its configuration to multiple KX II-101 devices.

➤ *To access the Backup/Restore page:*

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



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

➤ *To backup your KX II-101:*

1. Click Backup. A File Download dialog opens.
2. Click Save. A Save As dialog opens.
3. Choose the location, specify a file name, and click Save. A Download Complete dialog opens.

4. Click Close. The backup file is saved locally on your client machine with the name and location specified.

➤ *To restore your KX II-101:*

WARNING: Please 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 serial number, MAC Address, IP Address, name, etc. With this option, you can setup one KX II-101 and copy the configuration to multiple KX II-101 devices.
 - **Custom Restore.** With this option, you can select User and Group Restore, Device Settings Restore, or both. Select the appropriate checkboxes:
 - **User and Group Restore.** This option includes only user and group information. Use this option to quickly set up users on a different KX II-101.
 - **Device Settings Restore.** This option includes only device settings. Use this option to quickly copy the device information.
2. Click the Browse button. A Choose File dialog opens.
3. Navigate to and select the appropriate backup file and click Open. The file selected is listed in the Restore File field.
4. Click Restore. The configuration (based on the type of restore selected) is restored.

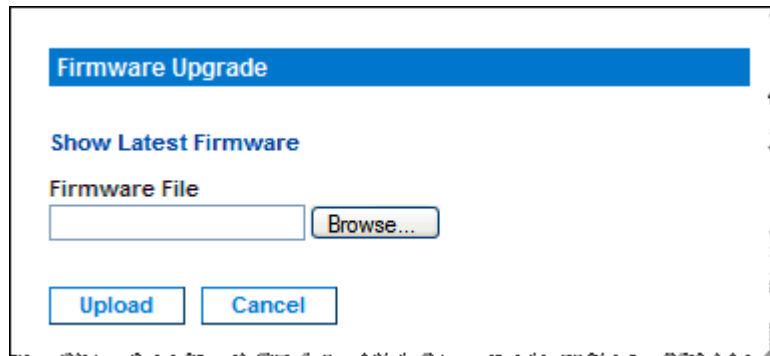
Firmware Upgrade

Use the Firmware Upgrade page to upgrade the firmware for your KX II-101 unit. This page is available in the KX II-101 Remote Console only.

Important: Do not turn off your KX II-101 unit while the upgrade is in progress - doing so will likely result in damage to the unit.

➤ *To upgrade your KX II-101 unit:*

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

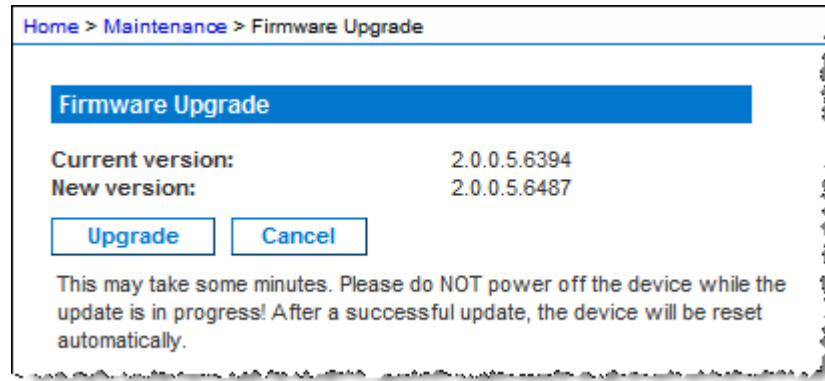


2. Click the Show Latest Firmware link, locate the appropriate Raritan firmware distribution file (*.RFP) from the Firmware Upgrades > KX II-101 page, and download the file.
3. Unzip the file and read all instructions included in the firmware ZIP files carefully before upgrading.

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.

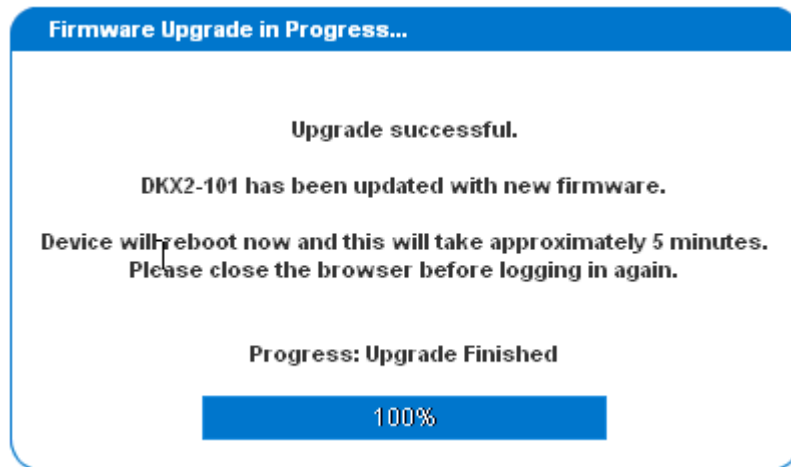
Firmware Upgrade

- 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 unit reboots.



- As prompted, close the browser and wait approximately 5 minutes before logging in to the KX II-101 again.

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

Upgrade History

KX II-101 provides information about upgrades performed on the KX II-101 unit and attached CIMS.

- *To view the upgrade history:*
 - Choose Maintenance > Upgrade History. The Upgrade History page opens:

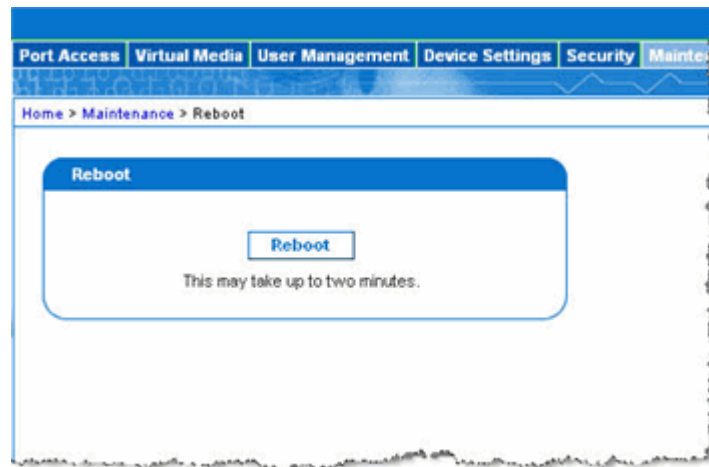
Type	User	IP	Start Time	End Time	Previous Version	Upgrade Version	Result
Full Firmware Upgrade	admin	192.168.50.67	January 09, 2000 20:30	January 09, 2000 20:32	2.0.0.5.6236	2.0.0.5.6236	Successful
Full Firmware Upgrade	admin	192.168.50.67	January 09, 2000 20:18	January 09, 2000 20:20	2.0.0.5.6191	2.0.0.5.6236	Successful
Full Firmware Upgrade	admin	192.168.50.65	January 06, 2000 17:58	January 06, 2000 18:01	2.0.0.1.6126	2.0.0.5.6191	Successful
Full Firmware Upgrade	admin	192.168.59.35	January 01, 2000 00:02	January 01, 2000 00:04	99.99.99.2.9999	2.0.0.1.6126	Successful
Full Firmware Upgrade	admin	192.168.59.35	January 01, 1970 00:06	January 01, 1970 00:09	2.0.0.1.5974	99.99.99.2.9999	Successful
Full Firmware Upgrade						2.0.0.1.5974	Failed

Reboot

The Reboot page provides a safe and controlled way to reboot your KX II-101 unit; this is the recommended method for rebooting.

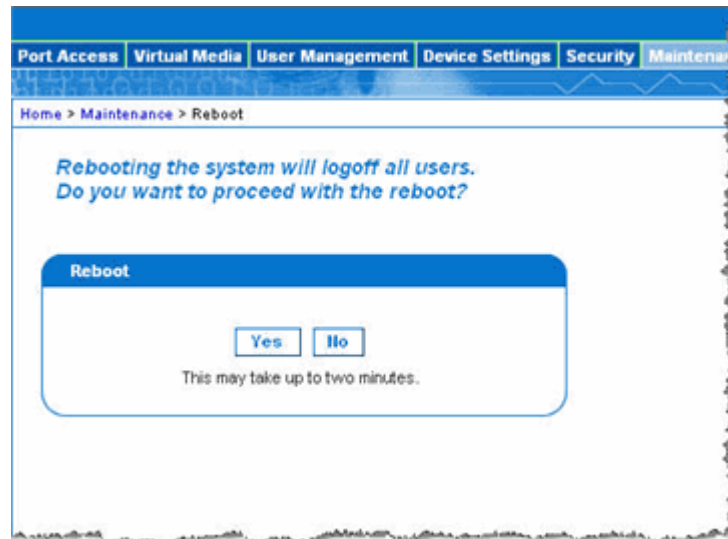
Important: All KVM and serial connections will be closed and all users will be logged off.

- *To reboot your KX II-101:*
 1. Choose Maintenance > Reboot. The Reboot page opens:



Reboot

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



3. Click Yes to proceed with the reboot.

➤ *To exit without rebooting:*

- Click No.

Chapter 12 Command Line Interface (CLI)

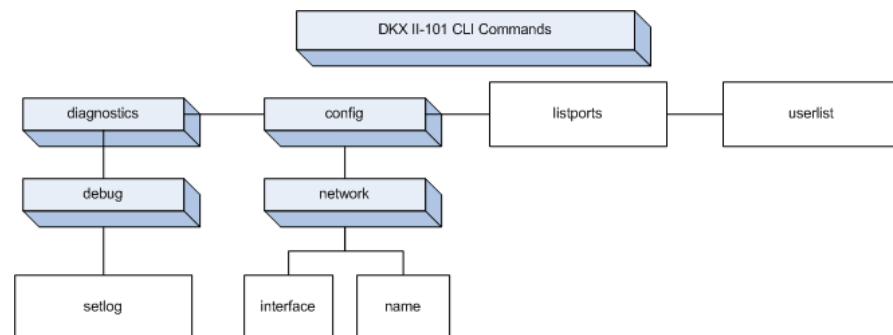
In This Chapter

Overview.....	163
Accessing the KX II-101 Using the CLI.....	164
SSH Connection to the KX II-101.....	164
Login.....	165
Navigation of the CLI.....	166
CLI Commands.....	168

Overview

This chapter provides an overview of the CLI commands that can be used with the KX II-101. See *CLI Commands* (on page 168) 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 by 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

A number of SSH/TELNET clients are available and can be obtained from the following locations:

- Putty - <http://www.chiark.greenend.org.uk/~sgtatham/putty/> (<http://www.chiark.greenend.org.uk/~sgtatham/putty/>)
- SSH Client from ssh.com - www.ssh.com (<http://www.ssh.com>)
- Applet SSH Client - www.netbeans.org/ssh (<http://www.netbeans.org/ssh>)
- OpenSSH Client - www.openssh.org (<http://www.openssh.org>)

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 120) for information.

SSH Connection to the KX II-101

Use any SSH client that supports SSHv2 to connect to it. You must enable SSH access from the Devices Services page. See *Device Services* (on page 120) for information.

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

SSH Access from a Windows PC

➤ *To open an SSH session from a Windows PC:*

1. Launch the SSH client software, such as PuTTY.
2. Enter the IP address of the KX II-101 server 192.168.0.192.
3. Choose SSH, which uses the default configuration port 22.
4. Click the Open button.
5. The following prompt appears:
login as:

See the Login section for login information.

SSH Access from a UNIX Workstation

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

```
ssh -l admin 192.168.30.222
```

The following prompt appears:

```
password:
```

See the Login section for login information.

Login

- *To log in, enter the user name admin as shown:*

```
Login: admin
```

The password prompt appears. Enter the default password: raritan

```
Password:
```

The welcome message displays. 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 166) section, you can perform the initial configuration tasks described in *Using the Admin Serial Console* (see "Using a Terminal Emulation Program" on page 27).

Navigation of the CLI

Before using the CLI, it is important to understand CLI navigation and syntax. Additionally, there are combinations of keystrokes that simplify CLI use.

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 Port > Config > Network >
```

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

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

Completion of Commands

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

- If no match is found, the CLI displays the valid entries for that level.
- If greater than one possible match is found, the CLI also displays the valid entries.
- The user can enter additional text to make the entry unique and the Tab key to complete the entry.

CLI Syntax -Tips and Shortcuts

Tips

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

Shortcuts

- Press the Up-Arrow to display the last entry.
- Use the Backspace key to delete the last character typed.
- Use Ctrl/C to terminate a command or cancel a command if you typed the wrong parameters.
- Use Enter to execute the command.
- Press Tab to complete a command, such as:

Admin Port > Conf

The system 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.
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.
<i>diagnostics</i> (on page 169)	Switch to the diagnostics menu.
<i>debug</i> (on page 169)	Switch to debug menu.
help	Display an overview of the CLI syntax.
history	Display the current session's command line history.
interface	Configure the KX II-101 network interface.
<i>listports</i> (see "Listports Command" on page 172)	Lists the port, port name, port type, port status, and port availability.
logout	Logout of the current CLI session.
<i>name</i> (see "Name Command" on page 171)	Sets the device name.
<i>network</i> (on page 170)	Displays network configuration and enables you to configure network settings.
quit	Return to previous command.
<i>setlog</i> (see "Setlog Command" on page 169)	Sets device logging options.
top	Return to the root menu.
<i>userlist</i> (see "Userlist Command" on page 172)	Lists the number of active users, user names, port, and status.

Diagnostics

The Diagnostics menu enables you to set the logging options for different modules of the KX II-101. You should set logging options only when instructed by a Raritan Technical Support engineer. These logging options enable a support engineer to get the right kind of information for debugging and troubleshooting purposes. When instructed by a support engineer, you will be told how to set logging options and how to generate a log file to send to Raritan technical support.

Important: Set logging options only under the supervision of a Raritan Technical Support engineer.

Debug

The Diagnostics > Debug menu enables you to choose the Setlog command to set logging options for the KX II-101.

Setlog Command

The Setlog command enables you set the logging level for different modules of the KX II-101 and to view the current logging levels for each module. The syntax for the setlog command is:

```
setlog [module <module>] [level <level>] [vflag <vflag>]
[verbose <on|off>]
```

```
Set/Get diag log level
```

The Setlog command options are described in the following table. Raritan Technical Support will tell you how to configure these settings.

Command Option	Description
module	The module name.
level	The diagnostics level: err warn info debug trace

CLI Commands

Command Option	Description
vflag	The type of verbose flag: timestamp module thread fileline
verbose [on off]	Turns verbose logging on and off.

Setlog Command Example

The following Setlog command sets the logging level to debug with verbose logging on for the libpp_serial module.

```
Setlog module libpp_serial level debug verbose on
```

Configuration

The Configuration menu enables you to access the network commands used to configure the network interface and set the device name.

Network

The Configuration > Network commands are used to configure the KX II-101 network connection and device name.

Command	Description
interface	Configure the KX II-101 unit network interface.
name	Set the device name.

Name Command

The name command is used to configure the device and host name.

The syntax for the device name is:

```
name devicename <>
```

The syntax for the host name is:

```
name hostname <>
```

name Command Example

The following command sets the device name:

```
Admin Port > Config > Network > name devicename <device name>
```

The following command sets the host name:

```
Admin Port > Config > Network > name hostname <host name>
```

Interface Command

The interface command is used to configure the KX II-101 network interface. When the command is accepted, the unit 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) for information.

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 100Mbps full duplex (100fdx)

CLI Commands

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 No.	Port Name	Port Type	Port Status	Port 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 13 Diagnostics

In This Chapter

Diagnostics Menu	173
Network Interface Page	174
Network Statistics Page	174
Ping Host Page	177
Trace Route to Host Page	178
Device Diagnostics	179

Diagnostics Menu

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; the information displayed is the output of those commands.

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

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

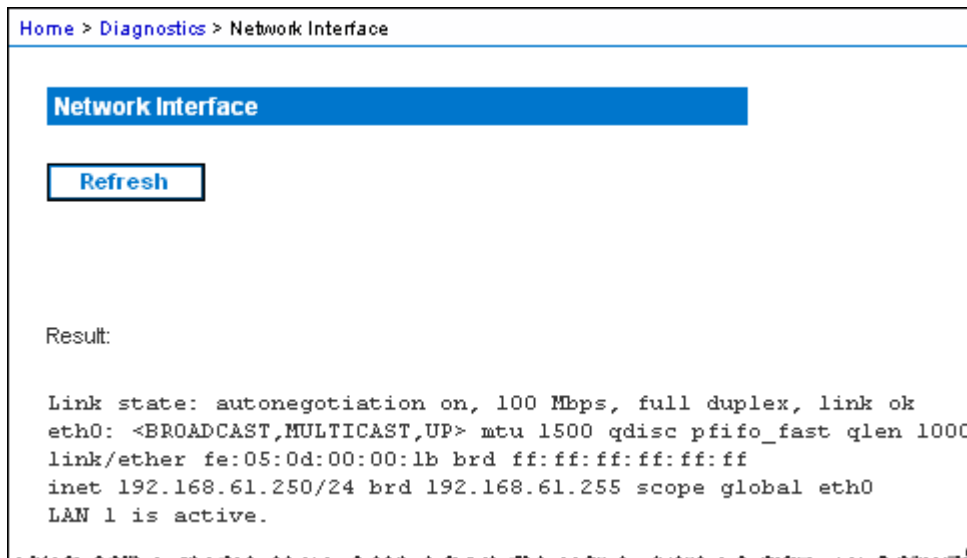
The Device Diagnostics option is intended for use in conjunction with Raritan Technical Support.

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

Network Interface Page

The 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 ping-able 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:

Port Access Virtual Media User Management Device Settings Security

Home > Diagnostics > Network Statistics

Network Statistics

Options:

Result:

```

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

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

Port Access Virtual Media User Management Device Settings Security Maintenance Diagnostics

Home > Diagnostics > Network Statistics

Network Statistics

Options:

Result:

```

Kernel Interface table
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth1 1500 0 13828 0 0 0 8680 0 0 0 B1NRU
lo 16436 0 196 0 0 0 196 0 0 0 LRU
  
```

Network Statistics Page

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

The screenshot shows a web interface with a blue header bar containing navigation tabs: Port Access, Virtual Media, User Management, Device Settings, Security, and Maint. Below the header, a breadcrumb trail reads 'Home > Diagnostics > Network Statistics'. The main content area has a blue title bar 'Network Statistics'. Underneath, there is an 'Options:' section with a dropdown menu showing '--route' and a 'Refresh' button. Below this is a 'Result:' section displaying the 'Kernel IP routing table' as a text-based table.

Destination	Gateway	Genmask	Flags	MSS	Window	irrtt	Iface
192.168.59.0	*	255.255.255.0	U	0	0	0	eth1
default	192.168.59.126	0.0.0.0	UG	0	0	0	eth1

3. Click the Refresh button.

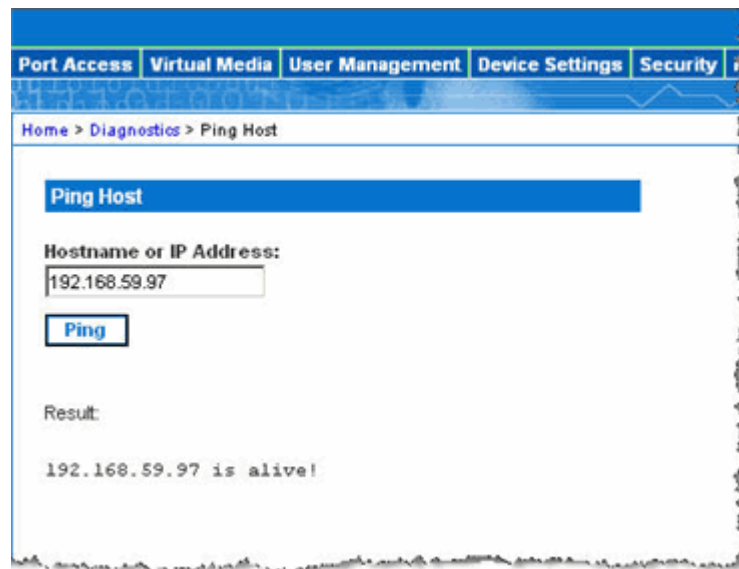
The relevant information is displayed in the Result field.

Ping Host Page

Ping is a network tool used to test whether a particular host or IP Address is reachable across an IP network. Using the Ping Host page, you can determine if a target server or another KX II-101 unit is accessible.

➤ *To ping the host:*

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



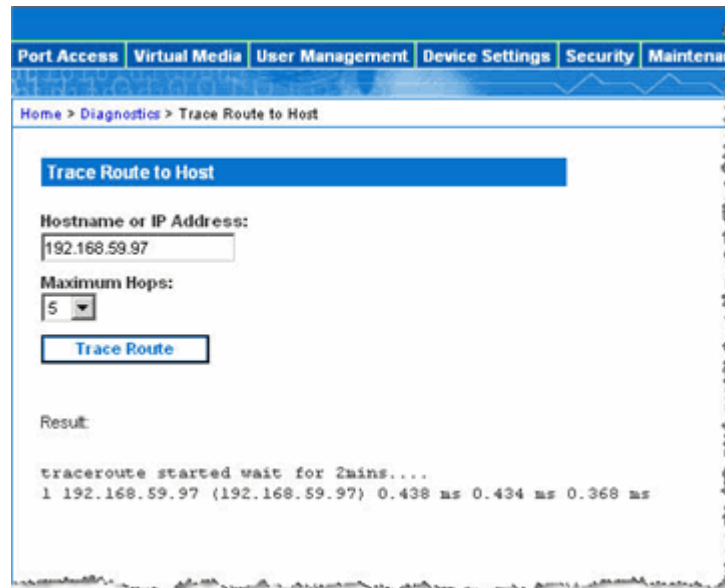
2. Type either the hostname or IP Address into the Hostname or IP Address field.
3. Click Ping. The results of the ping are displayed in the Result field.

Trace Route to Host Page

Trace Route is a network tool used to determine the route taken all the way to the provided hostname or IP Address.

➤ *To trace the route to the host:*

1. Choose Diagnostics > Trace Route to Host. The Trace Route to Host page opens:



The screenshot shows a web interface for 'Trace Route to Host'. At the top, there is a navigation bar with tabs: Port Access, Virtual Media, User Management, Device Settings, Security, and Maintenance. Below this is a breadcrumb trail: Home > Diagnostics > Trace Route to Host. The main content area has a title 'Trace Route to Host' in a blue box. Below the title, there is a form with two fields: 'Hostname or IP Address:' with a text input containing '192.168.59.97', and 'Maximum Hops:' with a dropdown menu set to '5'. A 'Trace Route' button is located below these fields. Under the 'Result:' label, the output of the trace route is displayed in a monospaced font: 'traceroute started wait for 2mins....' followed by '1 192.168.59.97 (192.168.59.97) 0.438 ms 0.434 ms 0.368 ms'.

2. Type either the Hostname or IP Address into the Hostname or IP Address field.
3. Choose the Maximum Hops from the drop-down list (5 to 50 in increments of 5).
4. Click the Trace Route button. The trace route command is executed for the given hostname or IP Address and the maximum hops. The output of trace route is displayed in the Result field.

Device Diagnostics

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

The Device Diagnostics page downloads diagnostics information from 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 (optional).** Loads a special script provided by Raritan Technical Support during a critical error debugging session. The script is uploaded to the unit and executed.
- **Device Diagnostic Log.** Downloads a snapshot of diagnostics messages from the KX II-101 unit to the client. This encrypted file is then sent to Raritan Technical Support; only Raritan can interpret this file.

Note: This page is accessible only by users with administrative privileges.

➤ *To run the KX II-101 System diagnostics:*

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

Home > Diagnostics > Device Diagnostics

Device Diagnostics

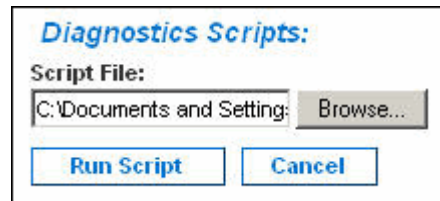
Diagnostics Scripts:

Script File:

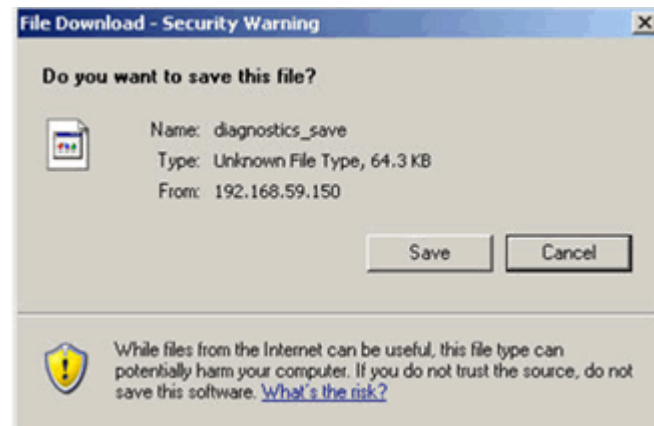
Dominion KX2-101 Diagnostic Log:

Device Diagnostics

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. Use the Browse button. A Choose File dialog opens.
 - c. Navigate to and select this diagnostics file.
 - d. Click Open. The file is displayed in the Script File field:



- e. Click Run Script.
3. Create a diagnostics file to send to Raritan Technical Support:
 - a. Click the Save to File button. The File Download dialog opens:



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

Chapter 14 CC Unmanage

In This Chapter

Overview.....	181
Removing KX II-101 from CC-SG Management.....	182
Using CC-SG in Proxy Mode	183

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 is displayed (after entry of a valid username and password):

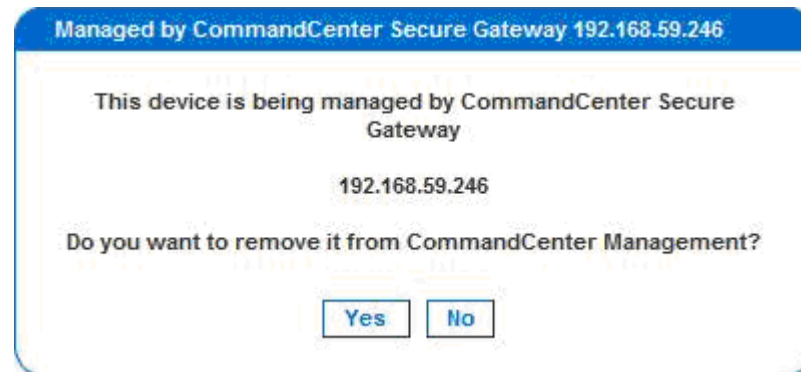


Removing KX II-101 from CC-SG Management

Unless the KX II-101 is released from CC-SG control, you cannot access the device directly. If, however, the KX II-101 does not receive heartbeat messages from CommandCenter (e.g., 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 is displayed when attempting to access the device directly:

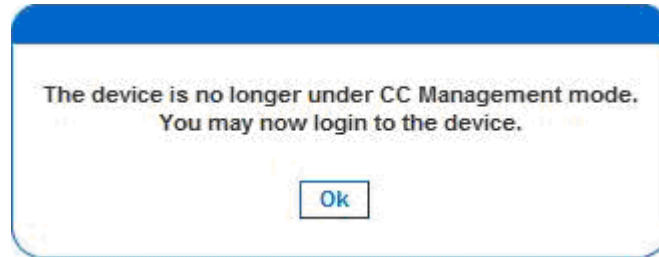


➤ To remove the device from CC-SG management (to use CC Unmanage):

1. Click the Yes button. You are prompted to confirm the action:



2. Click the Yes button. A message is displayed confirming that the device is no longer under CC management:



3. Click Yes. 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.....	184
Connectors	185
Raritan Remote Client Software	185

KX II-101

Form Factor	Zero U form factor; rack mountable vertically or horizontally (bracket kit included)
Dimensions (DxWxH)	4.055"x 2.913"x 1.063"; 103 x 74 x 27mm
Weight	0.6292lbs; 0.286kg
Power	AC/DC (100-240V~/ 6VDC) power adapter or Power over Ethernet (PoE) Mid-Span Power Insertion Signal-Pair Power Insertion
Operating temperature	0° - 40°C (32° - 104°F)
Humidity	20% - 85% RH
Indicators: Blue RARITAN back-lit logo Network Port	Boot-up and power-level indicator Network activity and connection speed indicator
Local connection	1- Mini USB port for USB keyboard / mouse and virtual media connectivity to the target 1- MiniDIN9 port for multi-function serial port of full RS-232 features, modem connection, and Dominion PX connectivity

Remote Connection: Network Protocols	One 10/100 Ethernet (RJ45) port TCP/IP, HTTP, HTTPS, UDP, RADIUS, LDAP, SNMP, DHCP
Screen Resolutions: PC graphic mode SUN® video mode	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:	UL/CUL, FCC Class A, CB, CE Class A and VCCI Class A

Connectors

Interface Type	Length (inch; cm)	Description
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

Raritan Remote Client Software

Operating System Requirements: Windows XP / NT / ME / 2000

Appendix B Rack Mount

The KX II-101 unit 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.

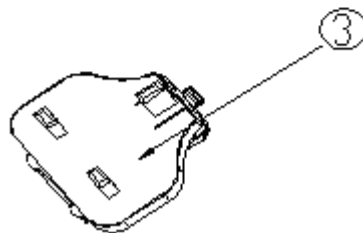
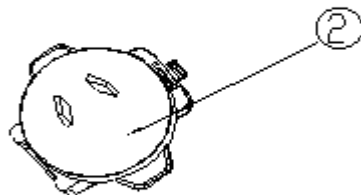
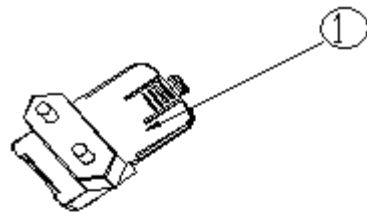
In This Chapter

AC-DC Adapter Clip Fitting	186
Bracket Installation	188

AC-DC Adapter Clip Fitting

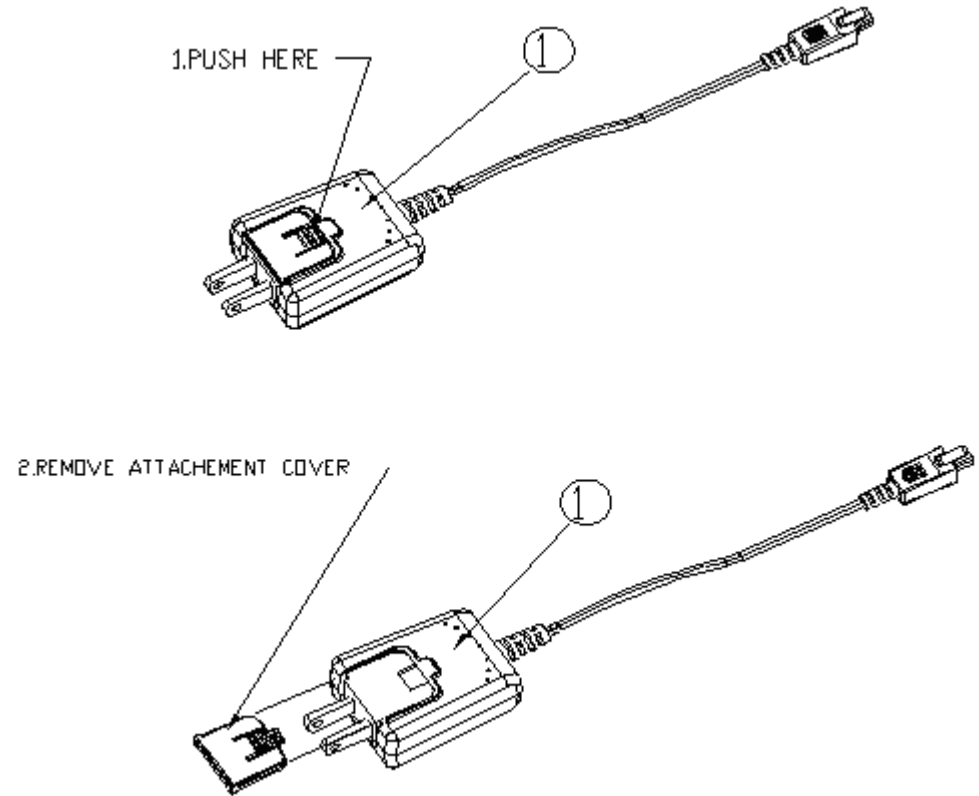
Identify Clip Type

1. EU Clip
2. Australian Clip
3. UK Clip



Remove Attachment Cover from AC-DC Power Adapter

1. AC/DC Power Adaptor
2. Attachment Cover

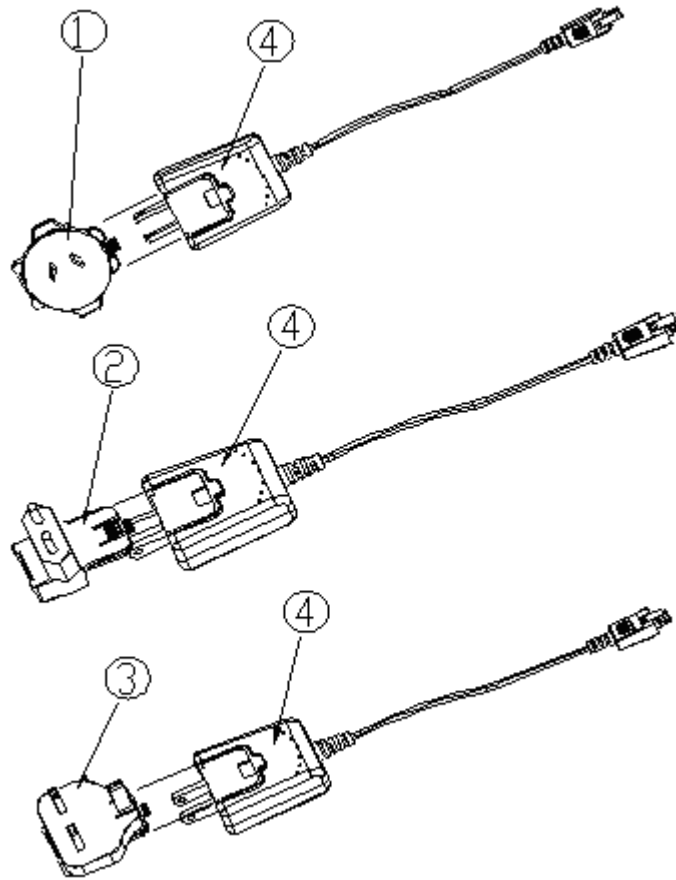


Attach Clip to AC-DC Power Adapter

1. Australian Clip
2. EU Clip
3. UK Clip

Bracket Installation

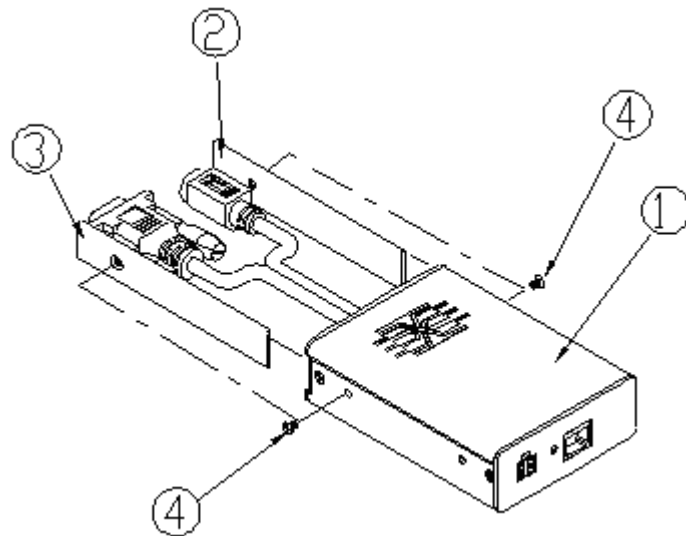
4. Power Adaptor



Bracket Installation

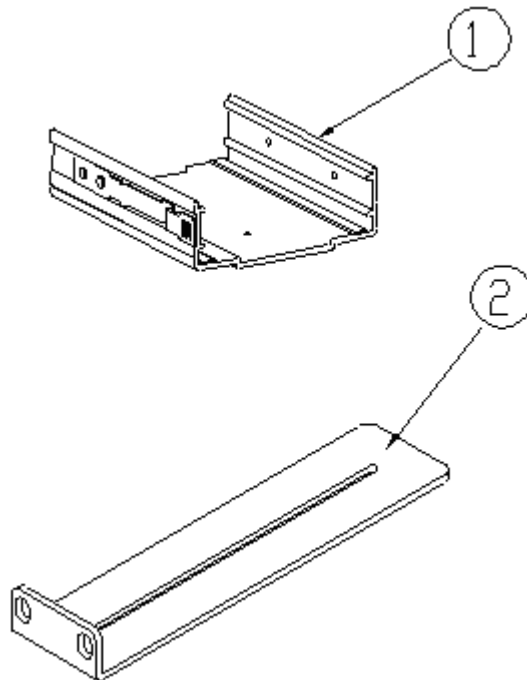
1. KX II-101 unit
2. Right panel
3. Left panel
4. Screws

- Remove the screws from the KX II-101 unit.
- Slide the left and right panels off the KX II-101 unit.



KX II-101 Bracket Parts

1. U Bracket
2. L Bracket

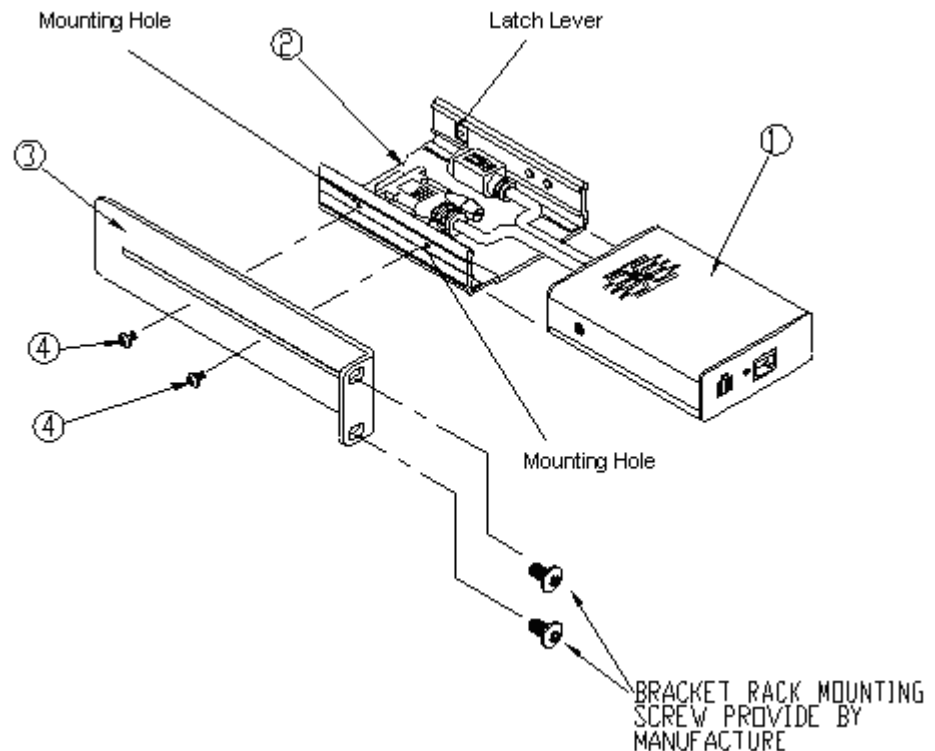


Bracket Installation

Attach Brackets to KX II-101 for Horizontal Mount

1. KX II-101 Unit
2. U Bracket
3. L Bracket
4. Screws
 - Attach the U Bracket to the L Bracket using the included screws. Adjust bracket placement before tightening screws.
 - Mount the U and L Bracket assembly to the rack with rack-mount screws (provided by the rack manufacturer).
 - Slide the KX II-101 unit into the U Bracket with the KVM harness facing towards the target. Pull and release the latch lever to lock the KX II-101 unit into the U Bracket.

The image below 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 unit.



Attach Brackets to KX II-101 for Vertical Mount

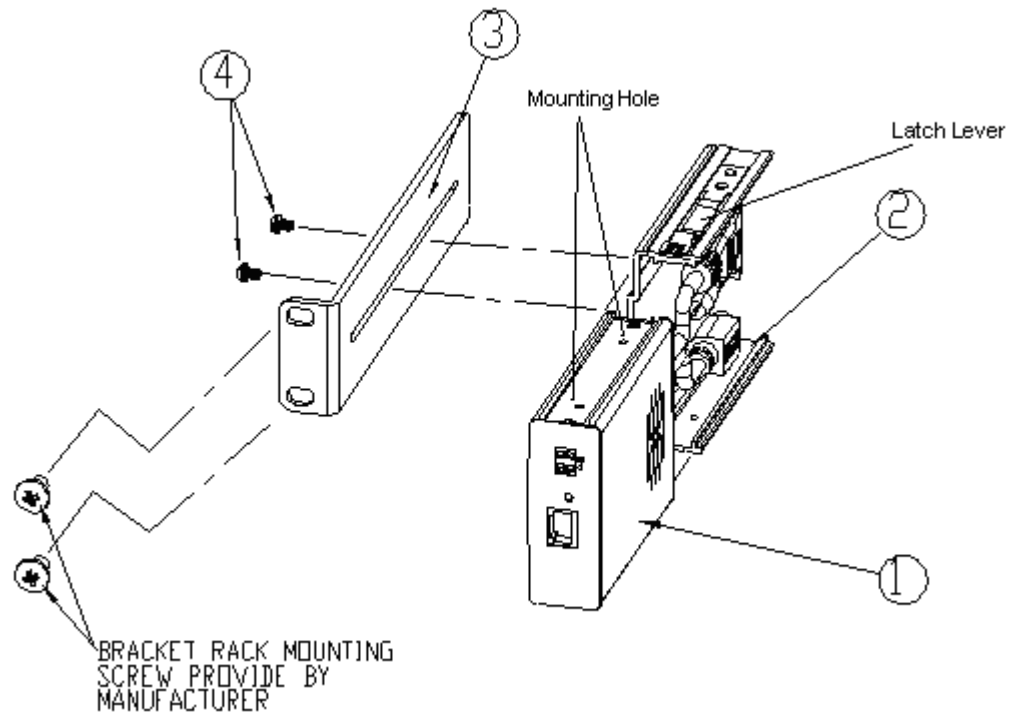
1. KX II-101 Unit

2. U Bracket
3. L Bracket
4. Screws

Attach the U Bracket to the L Bracket using the included screws. Adjust bracket placement before tightening screws.

Mount the U and L Bracket assembly to the rack with rack-mount screws (provided by the rack manufacturer).

Slide the KX II-101 unit into the U Bracket with the KVM harness facing towards the target. Pull and release the latch lever to lock the KX II-101 unit into the U bracket.



Index

A

- About Raritan Virtual KVM Client • 101
- Absolute • 98
- Accessing the KX II-101 Using the CLI • 164
- AC-DC Adapter Clip Fitting • 186
- Add New Favorite • 40, 45
- Add New User • 50, 52, 148
- Add New User Group • 54
- Adding Attributes to the Class • 72
- Administration Features • 4
- Apple® Macintosh Settings • 14
- Assigning an IP Address • 7, 23
- Associate KVM Target Servers to Outlets (Port Page) • 136, 141
- Attach Brackets to KX II-101 for Horizontal Mount • 190
- Attach Brackets to KX II-101 for Vertical Mount • 190
- Attach Clip to AC-DC Power Adapter • 187
- Audit Log • 155
- Authentication Settings • 60, 62
- Authentication vs. Authorization • 61, 62
- Auto-sense Video Settings • 92

B

- Backup and Restore • 157
- Blocking and Unblocking Users • 52
- Bracket Installation • 188

C

- Calibrate Color • 93
- CC Unmanage • 181
- CD-ROM/DVD-ROM/ISO Images • 106, 110, 112
- Change Password • 60
- Checking Your Browser for AES Encryption • 149, 151
- CLI Commands • 163, 168
- CLI Prompts • 166
- CLI Syntax -Tips and Shortcuts • 167
- Command Line Interface (CLI) • 163

- Common Commands for All Command Line Interface Levels • 167
- Completion of Commands • 166
- Conditions when Read-Write is not Available • 108, 109
- Configuration • 170
- Configuring Direct Port Access • 23
- Configuring Network Firewall Settings • 8, 21
- Configuring the KX II-101 • 8, 21
- Configuring the Target Server • 8
- Connect the Power Strip • 133, 137
- Connecting the KX II-101 • 8, 15
- Connecting to the KX II-101 • 24, 32
- Connecting to the Network • 20
- Connecting to the Target Server • 16
- Connecting to Virtual Media • 108
- Connection Info • 87
- Connection Menu • 85
- Connectors • 6, 185
- Control the Powerstrip Device • 133, 141
- Creating a Keyboard Macro • 89
- Creating a New Attribute • 71
- Creating Users and Groups • 25

D

- Date/Time Settings • 124
- Debug • 168, 169
- Default IP Address • 7
- Device Diagnostics • 179
- Device Information • 156
- Device Management • 114
- Device Services • 120, 164
- Device Settings Menu • 114
- Diagnostics • 168, 169, 173
- Diagnostics Menu • 173
- Disconnecting Virtual Media • 106, 111
- Discover Devices - KX II-101 Subnet • 44
- Discover Devices - Local Subnet • 42
- Displaying the Outlet Associations • 140
- Dominion KX II-101 Overview • 2

E

- Editing rcusergroup Attributes for User Members • 75
- Enabling Direct Port Access • 34
- Encryption and Share • 148
- Event Management • 125
- Event Management - Destinations • 128
- Exit • 87

F

- Favorites List • 40
- File Server Setup (File Server ISO Images Only) • 106, 112
- Firmware Upgrade • 159
- From LDAP • 70
- From Microsoft Active Directory • 70

G

- Group-based IP ACL (Access Control List) • 57
- Groups • 47

H

- Help Menu • 101

I

- Identify Clip Type • 186
- Implementing LDAP Remote Authentication • 64
- Implementing RADIUS Remote Authentication • 63, 67
- Important Information • 7
- Installation and Configuration • 8, 171
- Intelligent • 98
- Interface Command • 171
- Interfaces • 4
- Introduction • 1
- IP Access Control • 55, 57, 119, 151

J

- Java Runtime Environment (JRE) • 32

K

- Keyboard Macros • 88
- Keyboard Menu • 88
- Keyboard/Mouse Settings • 122
- KX II-101 • 184
- KX II-101 Bracket Parts • 189
- KX II-101 Console Layout • 35
- KX II-101 Console Navigation • 36
- KX II-101 Remote Console Menu Map • 37

L

- LAN Interface Settings • 118
- Language Support • 32
- Launching the KX II-101 • 33
- Linux Settings • 13
- Listports Command • 168, 172
- Local Drives • 106, 108
- Logging Out • 37
- Login • 7, 165
- Login Limitations • 145

M

- Maintenance • 154
- Maintenance Menu • 154
- Manage Favorites Menu • 39
- Managing Favorites • 38
- Menu Tree • 81
- Modify Existing User • 50, 52
- Modify Existing User Group • 53, 59
- Modifying a Keyboard Macro • 91
- Mounting • 5
- Mouse Menu • 83, 96
- Mouse Modes • 11
- Mouse Pointer Synchronization • 83
- Mouse Synchronization Tips • 83

N

- Name Command • 168, 171
- Name the Power Strip (Port Page for Power Strips) • 135
- Naming the Target Server • 24
- Navigation of the CLI • 165, 166
- Network • 168, 170
- Network Basic Settings • 116

- Network Configuration • 4
- Network Interface Page • 174
- Network Settings • 115
- Network Statistics Page • 174
- Note on Microsoft Active Directory • 61
- Note to CC-SG Users • 61

O

- Opening a KVM Session • 107
- Optional Accessories • 6
- Options • 81, 99
- Overview • 80, 103, 133, 163, 181

P

- Package Contents • 6
- Ping Host Page • 177
- Port Access Page • 46
- Port Configuration • 131
- Power • 5
- Power Control • 133
- Powering the KX II-101 • 20
- Prerequisites for Using Virtual Media • 105, 106
- Product Features • 4
- Product Photos • 3
- Properties Dialog • 85
- PS/2 Configuration • 16

R

- Rack Mount • 5, 186
- RADIUS Communication Exchange
 - Specifications • 68
- Raritan Remote Client Software • 185
- Reboot • 161
- Refresh Screen • 92
- Relationship between Users and Groups • 48
- Remote Authentication • 61
- Remove Attachment Cover from AC-DC
 - Power Adapter • 187
- Removing a Keyboard Macro • 91
- Removing KX II-101 from CC-SG
 - Management • 182
- Returning User Group Information • 69
- Returning User Group Information from
 - Active Directory Server • 66

- Returning User Group Information via
 - RADIUS • 68

- Running a Keyboard Macro • 91

S

- Scaling • 100
- Security Settings • 143, 144
- Security Settings Menu • 143
- Send Ctrl+Alt+Delete • 88
- Serial Port Settings • 123
- Service Pack • 7
- Set Permissions for Individual Group • 51, 56
- Setlog Command • 168, 169
- Setting a New Password • 22
- Setting Permissions • 55, 59
- Setting Port Permissions • 56
- Setting Server Video Resolution • 9, 16
- Setting Sun Video Resolution • 9
- Setting the Registry to Permit Write
 - Operations to the Schema • 71
- Single Mouse Cursor • 97
- SNMP Agent Configuration • 126, 129
- SNMP Configuration • 126
- SNMP Trap Configuration • 126, 129
- Specifications • 184
- SSH Access from a UNIX Workstation • 165
- SSH Access from a Windows PC • 164
- SSH Connection to the KX II-101 • 164
- Standard • 97
- Strong Passwords • 60, 145, 146
- Sun Solaris Settings • 13
- Supported Protocols • 61
- Synchronize Mouse • 96
- Syslog Configuration • 127
- System Management Features • 4

T

- Target Screen Resolution • 101
- Terminology • 6
- Toolbar • 82
- Tools Menu • 99
- Trace Route to Host Page • 178

U

- Updating the LDAP Schema • 66, 69

Index

- Updating the Schema Cache • 74
- Upgrade History • 161
- USB Configuration • 18
- User Blocking • 52, 145, 147
- User Features • 5
- User Group List • 53
- User List • 49
- User Management • 49
- User Management Menu • 49
- Userlist Command • 168, 172
- Users • 47
- Users, Groups, and Access Permissions • 47
- Using a Terminal Emulation Program • 7, 27, 165
- Using CC-SG in Proxy Mode • 183
- Using the Admin Port • 20, 27
- Using the Local User Port • 21
- Using the Remote Console • 22
- Using Virtual Media • 106

V

- Video Menu • 92
- Video Resolution • 5
- Video Settings • 93
- View Menu • 100
- View Toolbar • 100
- Virtual KVM Client • 79
- Virtual Media • 98, 102

W

- Windows 2000 Settings • 12
- Windows Vista • 11
- Windows XP Settings • 12



➤ *U.S./Canada/Latin America*

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

➤ *China*

Beijing

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

Shanghai

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

GuangZhou

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

➤ *India*

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

➤ *Japan*

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5994
Email: support.japan@raritan.com

➤ *Europe*

Europe

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

United Kingdom

Monday - Friday
8:30 a.m. to 5 p.m. GMT+1 CET
Phone +44-20-7614-77-00
France
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0

➤ *Korea*

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +82-2-5578730

➤ *Melbourne, Australia*

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

➤ *Taiwan*

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