

**Dominion<sup>®</sup> KX101**

# User Guide

**Raritan Inc.**

400 Cottontail Lane  
Somerset, NJ 08873  
USA  
Tel. 1-732-764-8886  
Fax. 1-732-764-8887  
E-mail: [Hsales@raritan.com](mailto:Hsales@raritan.com)  
[Hhttp://www.raritan.com/H](http://www.raritan.com/H)

**Raritan Computer Japan, Inc.**

4th Flr. Shinkawa NS Building  
1-26-2 Shin-kawa, Chuo-ku  
Tokyo 104-0033  
Japan  
Tel. 81-03-3523-5991  
Fax. 81-03-3523-5992  
E-mail: [Hsales@raritan.co.jp](mailto:Hsales@raritan.co.jp)  
[Hhttp://www.raritan.co.jpH](http://www.raritan.co.jpH)

**Raritan Computer France**

120 Rue Jean Jaurès  
92300 Levallois-Perret  
France  
Tel. 33-14-756-2039  
Fax. 33-14-756-2061  
E-mail: [Hsales.france@raritan.comH](mailto:Hsales.france@raritan.comH)  
[Hhttp://www.raritan.frH](http://www.raritan.frH)

**Raritan Computer U.K. Ltd.**

36 Great St. Helen's  
London  
EC3A 6AP  
United Kingdom  
Tel. 44 20 7614 7700  
Fax. 44 20 7614 7701  
E-mail: [Hsales.uk@raritan.com](mailto:Hsales.uk@raritan.com)  
[Hhttp://www.raritan.comH](http://www.raritan.comH)

**Raritan Computer Europe, B.V.**

Eglantierbaan 16  
2908 LV Capelle aan den IJssel  
The Netherlands  
Tel. 31-10-284-4040  
Fax. 31-10-284-4049  
E-mail: [Hsales.europe@raritan.com](mailto:Hsales.europe@raritan.com)  
[Hhttp://www.raritan.com/H](http://www.raritan.com/H)

**Raritan Computer Taiwan, Inc.**

5F, 121, Lane 235,  
Pao-Chiao Rd., Hsin Tien  
Taipei Hsien  
Taiwan, ROC  
Tel. 886-2-8919-1333  
Fax. 886-2-8919-1338  
E-mail: [Hsales.asia@raritan.com](mailto:Hsales.asia@raritan.com)  
[Hhttp://www.raritan.com.twH](http://www.raritan.com.twH)

**Raritan Computer Deutschland GmbH**

Lichstraße 2  
D-45127 Essen  
Germany  
Tel. 49-201-747-9820  
Fax. 49-201-747-9850  
E-mail: [Hsales.germany@raritan.comH](mailto:Hsales.germany@raritan.comH)  
[Hhttp://www.raritan.deH](http://www.raritan.deH)

**Shanghai Representative Office of  
Raritan Computer, Inc.**

RM 17E, Cross Region Plaza  
899 Lingling Road  
Shanghai China 2000030  
Tel. 86-21-5425-2499  
Fax. 86-21-5425-3992  
E-mail: [Hsales.china@raritan.com](mailto:Hsales.china@raritan.com)  
[Hhttp://www.raritan.com.cnH](http://www.raritan.com.cnH)



Copyright ©2007 Raritan Computer, Inc.  
KX101-0B-E  
August 2007  
255-62-4003

---

*This page intentionally left blank.*

---

## 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.

## Trademark Information

© Copyright 2007 Raritan, Inc. Dominion, IP-Reach, Paragon, MasterConsole, and their respective logos are trademarks or registered trademarks of Raritan, Inc. All rights reserved. PS/2, RS/6000, and PC/AT are registered trademarks of International Business Machines Corporation. Sun is a registered trademark of Sun Microsystems. Microsoft and Windows are registered trademarks of Microsoft Corporation. Netscape and Netscape Navigator are registered trademarks of Netscape Communication Corporation. Mozilla and Firefox are trademarks or registered trademarks of the Mozilla Foundation. Safari is a registered trademark of Apple Computer, Inc. All other marks are the property of their respective owners.

## 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。

*For assistance in the U.S., please contact the Raritan Technical Support Team by telephone (732) 764-8886, by fax (732) 764-8887, or by e-mail [tech@raritan.com](mailto:tech@raritan.com)  
Ask for Technical Support – Monday through Friday, 8:00am to 8:00pm, Eastern.*

*For assistance internationally, please contact your regional Raritan office.*

---

## Important Information

### Login

- The default KX101 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

- KX101 ships with factory DHCP default. In a network without a DHCP server, the user will need to configure a static IP address, net mask, and gateway addresses via the KX101 serial admin console.

### Service Pack

- KX101 users with Microsoft Internet Explorer version 5.01 or Windows 2000 must upgrade to Service Pack 4 (SP4) or higher.

# Contents

Chapter 1: Introduction .....	1
Dominion KX101 Overview .....	1
Product Photos .....	1
Product Features .....	1
Package Contents .....	2
Terminology .....	3
Chapter 2: Installation .....	5
Rack Mounting .....	5
Attaching a PS2 or USB Harness Pigtail .....	5
Configuring Target Servers .....	5
Server Video Resolution .....	5
Windows XP Settings .....	5
Windows 2000 Settings .....	6
Linux Settings .....	6
Sun Solaris Settings .....	6
Configuring Network Firewall Settings .....	7
KX101 Physical Connections .....	7
Connecting the KX101 .....	8
KVM PS/2 Port .....	8
Admin Port .....	8
Power Port/LAN Port .....	8
LAN LED .....	8
Local Port .....	9
Initial Configuration .....	10
Navigating the Configuration Menus .....	11
Navigation Overview .....	11
Network Configuration .....	12
Time and Date .....	13
Administrator Password .....	14
Reset to Factory Default Settings .....	14
Restart or Shutdown .....	14
Diagnostics .....	15
Administrator Password .....	15
Chapter 3: Raritan Remote Client (RRC) .....	17
Invoking RRC via Web Browser .....	17
Client PC Video and Display Drivers .....	17
Security Settings .....	17
Launching RRC .....	17
Removing RRC from the Browser Cache .....	18
Raritan Multi-Platform Client (MPC) .....	19
Optional: Installing Standalone RRC Client .....	19
RRC Window Layout .....	20
RRC Navigator .....	20
Navigator Options .....	22
RRC Navigator – Display and Sorting Options .....	23
Creating New Profiles .....	27
Modifying Profiles .....	29
Deleting Profiles .....	29
Establishing a New Connection .....	29
Closing a Remote Connection .....	30
RRC Toolbar and Shortcuts .....	30
RRC Status Bar .....	31
Keyboard Shortcut Menu .....	32
Remote KVM Console Control .....	33
Single Mouse Mode / Dual Mouse Mode .....	34
Automatic Mouse Synchronization .....	35
Mouse Mode .....	35
Full Screen Mode .....	36
Scaling .....	37
Auto-Scroll .....	37

Keyboard Handler .....	37
Keyboard Macros .....	38
Connection and Video Properties .....	41
Color Calibration .....	44
Select Administrative Functions via RRC .....	45
Firmware Upgrade .....	45
Device Restart .....	45
Device Configuration Backup and Restore .....	45
User Configuration Backup and Restore .....	45
Log Files .....	45
Broadcast Port .....	46
Remote Power Management .....	46
General Options .....	46
Chapter 4: Administrative Functions .....	49
Launching Dominion KX Manager .....	49
KX Manager Interface .....	50
Network Configuration .....	51
System-Level Security Parameters .....	54
Time and Date .....	56
Users, Groups, and Access Permissions .....	57
Overview .....	57
Relationship between Users and Group Entries .....	57
Create or Edit User Groups and Access Permissions .....	58
Moving Users between Groups .....	61
Delete User Groups .....	61
Create or Edit Users .....	61
Delete Users .....	62
Remote Authentication .....	63
Introduction .....	63
Remote Authentication Implementation .....	63
General Settings for Remote Authentication .....	65
Forced User Logoff .....	72
View KX Unit Event Log (Status) .....	73
Rebooting the Device .....	73
Device Diagnostic Console .....	73
Device System Information .....	74
Configuration Backup and Restore .....	74
Performance Settings .....	74
PC Properties .....	75
Appendix A: Specifications .....	77
Remote Connection .....	77
Raritan Remote Client Software .....	77
KVM Input .....	77
KVM Harness .....	77
Local Console Port .....	77
Appendix B: KX101 Rack Mount .....	79
AC-DC Adapter Clip Fitting .....	79
Identify Clip Type .....	79
Remove Attachment Cover from AC-DC Power Adapter .....	80
Attach Clip to AC-DC Power Adapter .....	81
Bracket Installation .....	82
KX101 Bracket Parts .....	83
Attach Brackets to KX101 for Horizontal Mount .....	84
Attach Brackets to KX101 for Vertical Mount .....	85
KX101 FAQs Online .....	87

# Figures

Figure 1 KX101 Units .....	1
Figure 2 Mouse Motion Specification Screen.....	7
Figure 3 KX101 in Your Network.....	7
Figure 4 Top, Front, and Bottom Views of the KX101 .....	8
Figure 5 KX101 Connectivity including Local Port .....	9
Figure 6 KX101 Login Screen .....	10
Figure 7 KX101 Main Menu .....	11
Figure 8 KX101 Network Configuration Screen .....	12
Figure 9 KX101 Time and Date Screen .....	13
Figure 10 Admin Password Screen.....	14
Figure 11 RESET Confirmation Screen .....	14
Figure 12 KX101 Diagnostic Screen .....	15
Figure 13 Type the IP Address of your Dominion KX unit.....	17
Figure 14 RRC Loading Screen .....	18
Figure 15 Possible Security Alert Screens .....	18
Figure 16 RRC Screen Components .....	20
Figure 17 Expanded RRC Navigation Tree.....	21
Figure 18 View → Show Menu Options .....	23
Figure 19 Sort Ports by Channel.....	24
Figure 20 Navigator Displaying Ports in Channel Order .....	24
Figure 21 Sort Ports by Name.....	25
Figure 22 Navigator Displaying Ports in Name Order .....	25
Figure 23 Sort Ports by Status .....	26
Figure 24 Navigator Displaying Ports in Status Order.....	26
Figure 25 Connect tab .....	27
Figure 26 Compression Tab.....	28
Figure 27 Security tab.....	28
Figure 28 Modify Connection screen .....	29
Figure 29 RRC Toolbar .....	30
Figure 30 RRC Status Bar Components .....	31
Figure 31 RRC Keyboard Shortcut Menu .....	32
Figure 32 Navigation Tree.....	33
Figure 33 Remote Desktop, where dual mouse cursors will appear .....	34
Figure 34 Single Cursor Mode Confirmation Window .....	34
Figure 35 Full Screen Mode View .....	36
Figure 36 Auto-Scroll Border.....	37
Figure 37 Add Keyboard Macro Window .....	38
Figure 38 Add Keyboard Macro Window .....	39
Figure 39 Keyboard Macros Window .....	39
Figure 40 Minimize All Window Menu Option.....	40
Figure 41 Modify Connection Window .....	41
Figure 42 Settings Window .....	42
Figure 43 Example of Sizing the Notepad Window .....	44
Figure 44 RRC Options Panel.....	46
Figure 45 Single Cursor Mode Confirmation Screen.....	47
Figure 46 Dominion KX Manager Login Screen.....	49
Figure 47 KX Manager Main Screen.....	50
Figure 48 Network Configuration Window.....	51
Figure 49 Access Control List Window .....	52
Figure 50 Confirm Action Window.....	53
Figure 51 Security Configuration Window .....	54

Figure 52 Time and Date Settings .....	56
Figure 53 Add Group Window.....	58
Figure 54 Edit Group Window .....	59
Figure 55 Select Ports Window.....	60
Figure 56 Set Access Control List for Group Window .....	60
Figure 57 Add User Window .....	61
Figure 58 Edit User Window .....	62
Figure 59 Authorization Flow Diagram .....	64
Figure 60 Remote Authentication Window.....	65
Figure 61 Creating a New Attribute.....	67
Figure 62 Adding the Attributes to the Class.....	68
Figure 63 Entering the User Group Name to be Returned .....	69
Figure 64 ADSI Edit Window.....	69
Figure 65 User Properties Screen.....	70
Figure 66 Edit Attribute - adding user to KX group.....	70
Figure 67 Logoff User Menu Option.....	72
Figure 68 Status Log Window .....	73
Figure 69 Device Diagnostic Window .....	73
Figure 70 System Information Window (for Dominion KX).....	74
Figure 71 System Information Window (for KX101).....	74
Figure 72 Performance Settings Window.....	75
Figure 73 PC Properties Screen (shown on a Dominion KX with a Power Strip association) .....	76
Figure 74 Power Adapter Clips .....	79
Figure 75 Attachment Cover on AC-DC Power Adapter .....	80
Figure 76 Clip Attachment.....	81
Figure 77 Panel Removal.....	82
Figure 78 Bracket Parts .....	83
Figure 79 Attach Brackets to KX101 for Horizontal Mount.....	84
Figure 80 Attach Brackets to KX101 for Vertical Mount .....	85
Figure 81 PS2 and USB Pigtails .....	86



# Chapter 1: Introduction

## Dominion KX101 Overview

Thank you for purchasing Dominion KX101. The KX101 provides a single KVM port for connection to a target server and a single IP port for connection to an IP network. Within the KX101 unit, KVM signals from your server are converted to IP format and compressed for transmission over an IP network.

You can control the KX101 via Raritan's CommandCenter (v 2.2 and above), or operate KX101 independently via Raritan's KX Manager and RRC management software platforms.

The KX101 dongle form-factor makes it easy to install near the target server, and each individual KX101 unit has its own IP Address. Each unit is powered via Power-over-Ethernet (PoE) or optionally from an in-line power adaptor.

## Product Photos

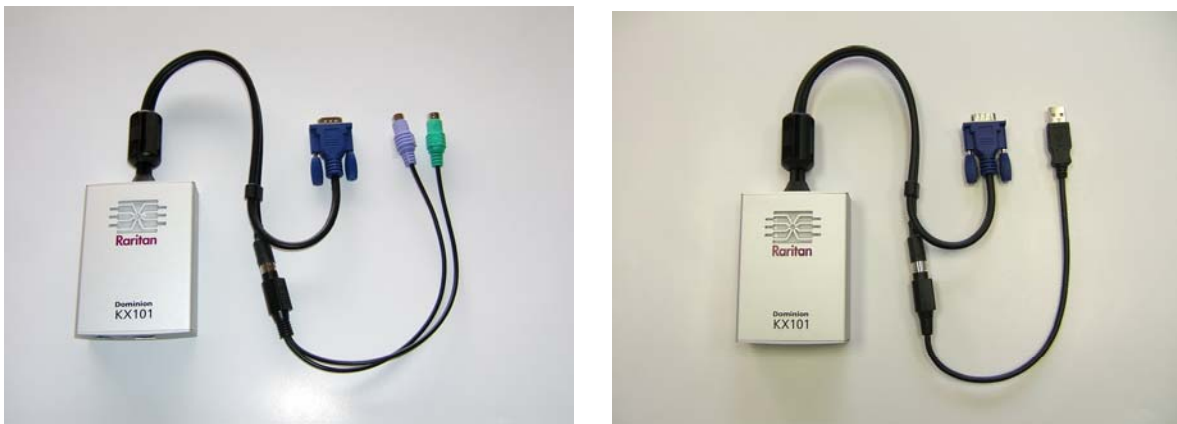


Figure 1 KX101 Units

## Product Features

### Interfaces

- Integrated KVM harness. PS/2 and USB is user interchangeable
- RJ11 serial Admin port for initial device setting and diagnostics
- 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

### Administration Features

- Full support and integration with CommandCenter 2.2
- KX Manager administration
- Raritan Remote Client (RRC)

### 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
- USB absolute mouse positioning
- Intelligent mouse synchronization

### **User Features**

- Internet Explorer browser connection.
- “PC Share” mode enabling more than one remote user.
- 128-bit SSL security
- TCP communication
- English User Interface

### **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

## **Package Contents**

Each KX101 unit ships with:

- Main Unit KX101 – KVM over IP Dongle
- Cable attachment PS2 / KX101
- Cable attachment USB / KX101
- Power Adaptor Kit – AC-DC 6VDC
- CRJ2DB20: CABLE MISC – RJ11 cable
- Changer A9F-RJ11 – Serial port adapter
- 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

<b><i>Target Server(s)</i></b>	Servers to be accessed remotely via KX101 and its connected KVM configuration.
<b><i>Remote PC</i></b>	A Windows-based computer used to access and control target servers connected to KX101.
<b><i>Serial Admin Console port</i></b>	The KX101 is provisioned with a local Serial Admin console port. Connect the serial port on the PC to the Serial Admin console port of the KX101 unit using the included RJ11 cable. Then use a standard emulation software package (e.g., Hyper Terminal) to access the Serial Admin console port. The serial admin console port is used for Network configuration, setting time and date, setting ADMIN password, viewing factory default settings, restart or shutdown, logging out, and Diagnostics.



## Chapter 2: Installation

### Rack Mounting

Please see **Appendix B: KX101 Rack Mount** for information on rack mounting the KX101 unit.

### Attaching a PS2 or USB Harness Pigtail

Prior to powering on the KX101 unit, align and attach the desired pigtail to the Mini-DIN-8 (circular) connector on the KX101 integrated harness. Please see **Appendix B: KX101 Rack Mount** for an illustration of the PS2 and USB pigtails.

### Configuring Target Servers

Before installing KX101, first configure any target servers that you wish to access via KX101, in order to ensure optimum performance, as outlined below. Note that the following configuration requirements apply only to *target servers*, not to the computers that you will be using to access KX101 remotely.

After KX101 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.

#### Server Video Resolution

---

For optimal bandwidth efficiency and video performance, target servers running graphical user interfaces 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 KX101, and that the signal is non-interlaced. KX101 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	

#### Windows XP Settings

---

On target servers 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 Target Servers running Windows 2000 or XP, you may wish to create a username to be used only for remote connections through KX101. This allows you to keep the Target Server's slow mouse pointer motion/acceleration settings exclusive to the KX101 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 KX101 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 KX101 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 target servers 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 target servers running Linux graphical interfaces, set the mouse acceleration to exactly 1 and set threshold to exactly 1.

As mentioned above, please ensure that each target server running Linux is using a resolution supported by KX101 at a standard VESA resolution and refresh rate. Each Linux target server should also be set so the blanking times are within +/- 40% of VESA standard values.

To check for these parameters:

- Go to the Xfree86 Configuration file XF86Config
- Using a text editor, disable all non-KX101 supported resolutions
- Disable the virtual desktop feature, which is not supported by KX101
- Check blanking times (+/- 40% of VESA standard).
- 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

---

All target servers must be configured to one of the display resolutions supported by KX101. The most popular supported resolutions for Sun machines are:

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

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

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

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

On target servers 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.

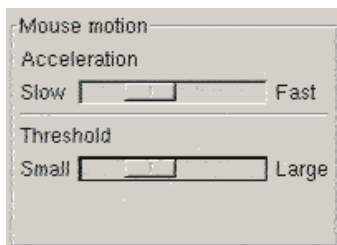


Figure 2 Mouse Motion Specification Screen

## Configuring Network Firewall Settings

To access KX101 through a network firewall, your firewall must allow communication on TCP Port 5000. Alternatively, KX101 can be configured to use a different TCP port of your own designation (see **Chapter 4: Administrative Functions, Network Configuration**).

In order to take advantage of KX101'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 KX101's redirection of HTTP requests to HTTPS (so that users may type the more common, "http://xxx.xx.xxxx", instead of "https://xxx.xx.xxxx"), then the firewall must allow inbound communication on TCP Port 80 – the standard TCP port for HTTP communication.

## KX101 Physical Connections

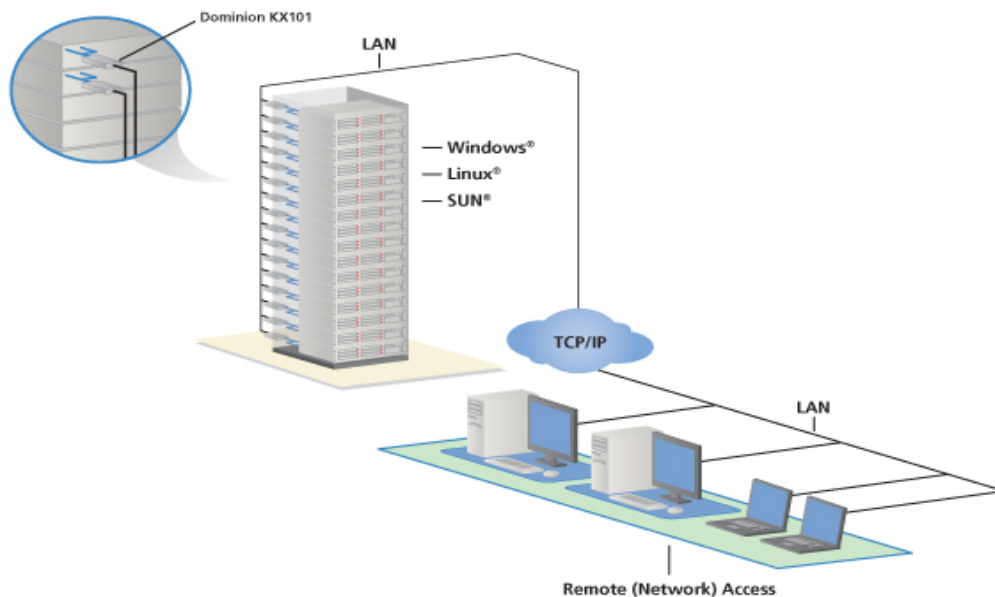


Figure 3 KX101 in Your Network

## Connecting the KX101

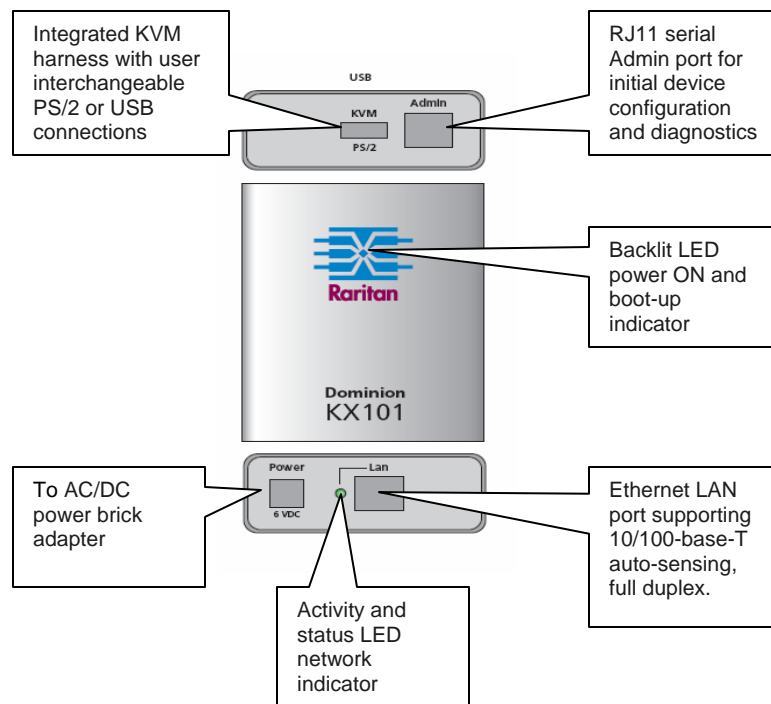


Figure 4 Top, Front, and Bottom Views of the KX101

### KVM PS/2 Port

The KX101 has a built-in harness with both USB and PS/2 pigtail attachments that originates from the KVM/PS/2 port.

### Admin Port

Plug the included RJ11 cable into the ADMIN port and plug the other end into the included A9F-RJ11 serial port adaptor in order to connect the KX101 unit to your PC or laptop.

### Power Port/LAN Port

KX101 can be powered either via 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 10/100BT cable to the LAN port, and plug the other end into a PoE-provisioned LAN.

### LAN LED

The LAN LED indicates Ethernet activity and blinks while the KX101 is in use.



## Local Port

**Note:** For local video access to target servers, use the optional LVC-101 cable.

The LVC-101 is an additional cable that can be ordered separately for the Dominion KX101 to provide local video access to the target server. The LVC-101 cable connects directly to the target server and local video monitor, providing local video functionality. Local mouse and keyboard control can be achieved by connecting a mouse and keyboard directly to the target server. This can be done through an unused pair of USB ports on the target server, or the PS/2 ports if they are not already in use by the KX101.

The LVC-101 comes equipped with one HD15M (male VGA) connector and 2 HD15F (female VGA) connectors, one labeled OUTPUT A, the second labeled OUTPUT B.

### To connect the LVC-101 cable:

1. Connect the HD15M connector into the Video Out port on the target server.
2. Connect the OUTPUT B HD15F connector to the HD15M connector on the KX101.
3. Connect the OUTPUT A HD15F connector to the local monitor.

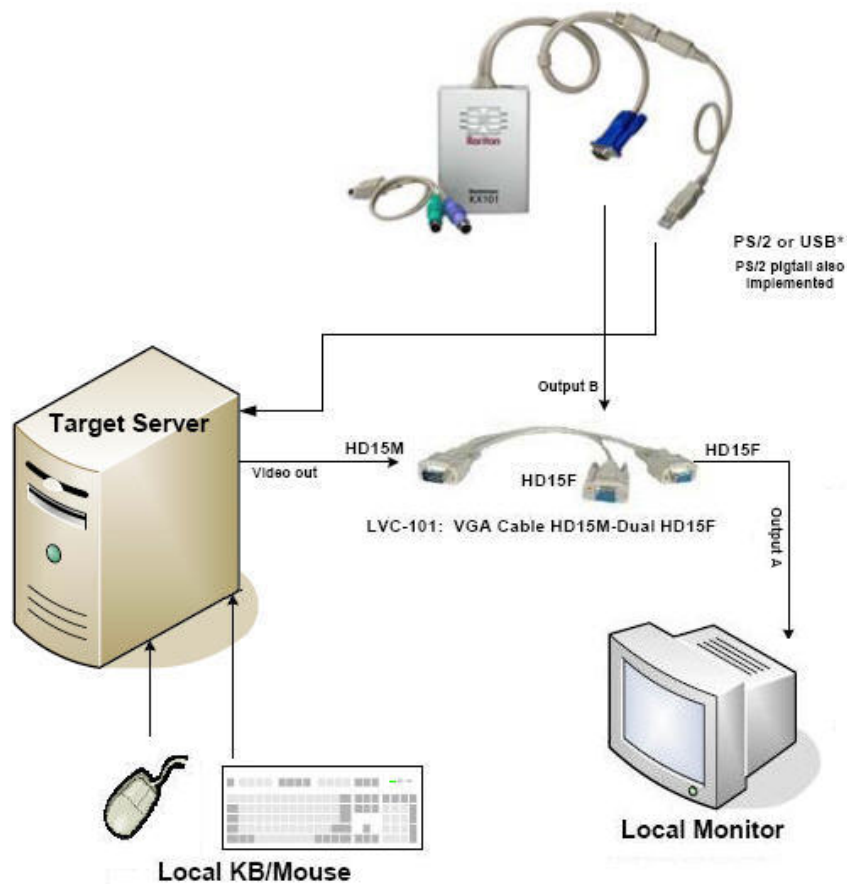


Figure 5 KX101 Connectivity including Local Port

## Initial Configuration

The easiest way to perform initial configuration on KX101 is using the Local Admin Console you connected to when following the **Physical Connection** instructions in the previous section.

1. Once you plug in the KX101, it powers ON, and the KX101 Login Screen appears on the Local Admin Console.

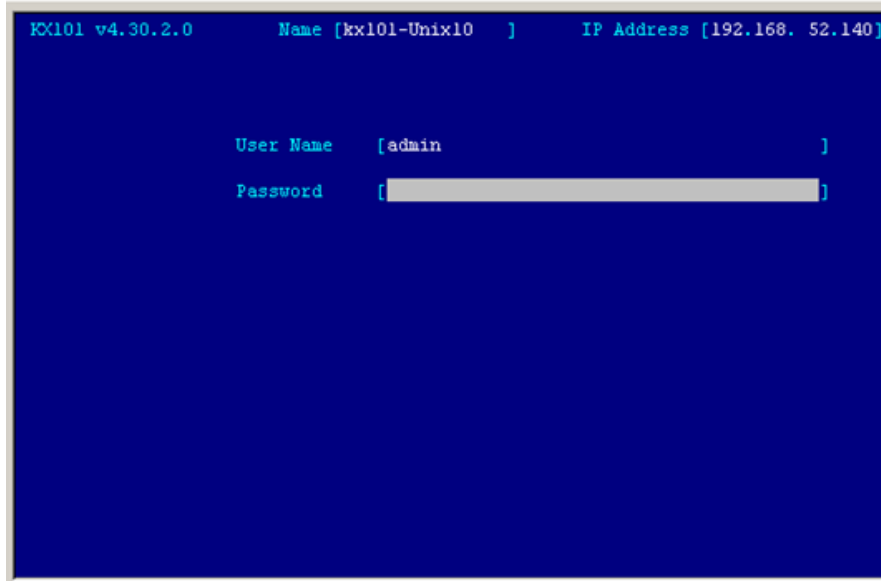


Figure 6 KX101 Login Screen

2. The default **User Name** is **admin** and cannot be changed.
3. Type your password in the **Password** field.
4. Press the **Enter** key on your keyboard to log on to KX101.

## Navigating the Configuration Menus

```
KX101 v4.30.2.0      Name [kx101-Unix10  ]      IP Address [192.168. 52.140]

                        - Main Menu -

[N] Network Configuration
[T] Time and Date
[P] Set ADMIN Password
[F] Reset to Factory Default Settings
[R] Restart or shutdown the KX101
[X] Logout
[D] Diagnostics

Press TAB to move to an option and ENTER to select the option.
```

Figure 7 KX101 Main Menu

### Navigation Overview

---

- Use the **Tab**, **↑**, **↓**, or letter keys on the keyboard to highlight the menu selection, then press the **Enter** key to execute.
- Press **Ctrl+S** to save changes. You may need to reboot the unit to apply the changes to the system.
- Press the **ESC** key to go back one screen.

## Network Configuration

On the Main Menu, select **[N] Network Configuration** (use the **↑** or **↓** keys or the letter N) and press **Enter** to edit network configuration values.

```

KX101 v4.30.2.0      Name [kx101-Unix10 ]      IP Address [192.168. 52.140]

- Network Configuration -

Name                [kx101-Unix10 ]

Enable Ethernet Interface [YES]
Line Speed & Duplex      [Auto Detect  ]
Obtain IP address automatically (DHCP) [YES]

Enable Web Browser Interface [YES]
Use Default TCP Port 5000    [YES]

CTRL+S - Save Changes  ESC - Cancel Changes  TAB - Next Field

```

Figure 8 KX101 Network Configuration Screen

- Use the **Tab**, **↑** or **↓** keys to navigate through the fields and the **space bar**, or the **←** or **→** keys to toggle between available entries. Press the **Enter**, **Tab** or **↓** keys when your entry on each line is complete. Below are descriptions of each field, and the appropriate values to assign.
  - Name:** Designate a unique name for this KX101 unit, for example, “Miami Data Center.” The default name is **KX101**. Please note: Only alphanumeric characters are supported and no name can begin with a numerical character; the only special characters supported are dashes and under-scores.
  - Enable Ethernet Interface:** Designates whether KX101 should enable its Ethernet adapter as active (default: YES).

---

**Note:** Network connections must be 10BASE-T or 100BASE-T Ethernet

---

- **Line Speed & Duplex:** Enter the visual efficiency for the monitor: Auto detect, 10 Mbps/Full Duplex, 10 Mbps/Half Duplex, 100 Mbps/Full Duplex, or 100 Mbps/Half Duplex
- **Obtain IP address automatically (DHCP):**
  - ◆ **YES (default):** Enables dynamic IP addressing for KX101. Each time KX101 boots, it requests an IP address from the local DHCP server. Note that this setting can make remote access to KX101 from outside the LAN difficult, since the dynamically assigned IP address must be known in order to initiate a connection.
  - ◆ **NO:** Assigns a fixed IP address to the KX101 unit (recommended).
    - **IP Address:** Enter the IP address for KX101 given by your Network Administrator.
    - **Subnet Mask:** Enter a Subnet Mask provided by your Network Administrator.
    - **Default Gateway:** Enter the Default Gateway if your Network Administrator specifies one.
- **Enable Web Browser Interface:** Enables Web browser access to KX101 (default: YES).

- **Use Default TCP Port 5000:**
  - **YES (default):** Utilizes the default port 5000.
  - **NO:** Enter an alternate port number.

---

*Note: In order to access KX101 from beyond a firewall, your firewall settings must enable two-way communication through the default port 5000 or the non-default port configured above.*

---

2. Press **Ctrl+S** to save entries and return to the Main Menu.
3. On the Main Menu, select **[R] Restart or shutdown the KX101**, and press the **Enter** key.
4. When prompted, press the letter **R** on your keyboard to restart KX101.
5. KX101 will restart and the KX101 Initialization screen appears upon boot up. KX101 is now ready for initial connection.

## Time and Date

On the Main Menu, select **[T] Time and Date** to set Current Time and Date or to adjust for daylight savings time. Changes to time and date will not take effect until the KX101 is restarted.

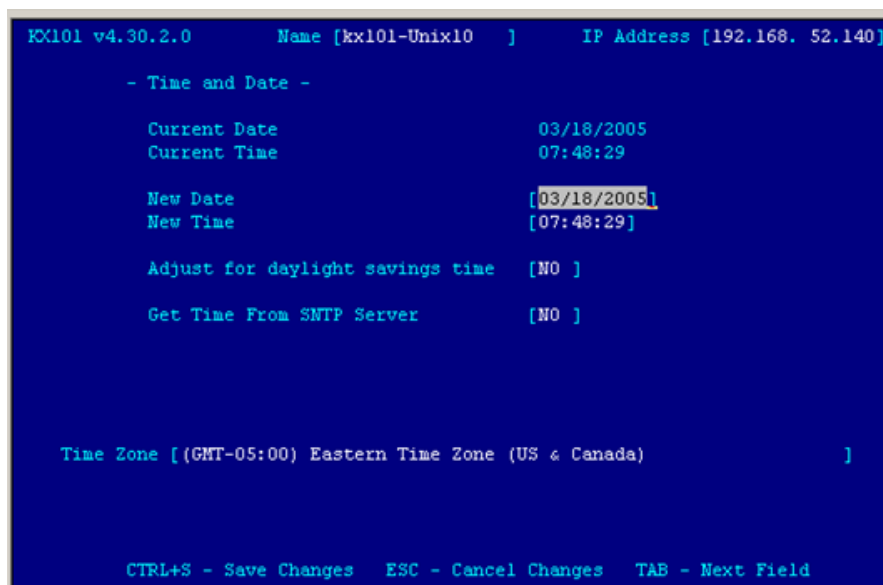


Figure 9 KX101 Time and Date Screen

- **New Date / New Time:** To manually input changes to current date and time values.
- **Adjust for daylight savings time:** Toggle between YES and NO to reflect whether your country or state follows the daylight savings time procedure.
- **Get Time From SNTP Server:** Indicates whether KX101 time/date should be automatically synchronized with the time/date of an external SNTP server.
  - **Primary Server IP Address:** IP address of first SNTP server to attempt time synchronization.
  - **Secondary Server IP Address:** IP address of second SNTP server to query, if primary server is unavailable.
  - **User standard UDP port 123:** Allows user to modify UDP port used for SNTP time synchronization. Consult your SNTP server administrator to determine if this value should be adjusted.

- **Time Zone:** Select the time zone in which your KX101 unit is physically located. Press <Ctrl+S> to save changes or <Esc> to cancel changes, and return to the Configuration Menu. Saved changes will not take effect until KX101 is restarted.

## Administrator Password

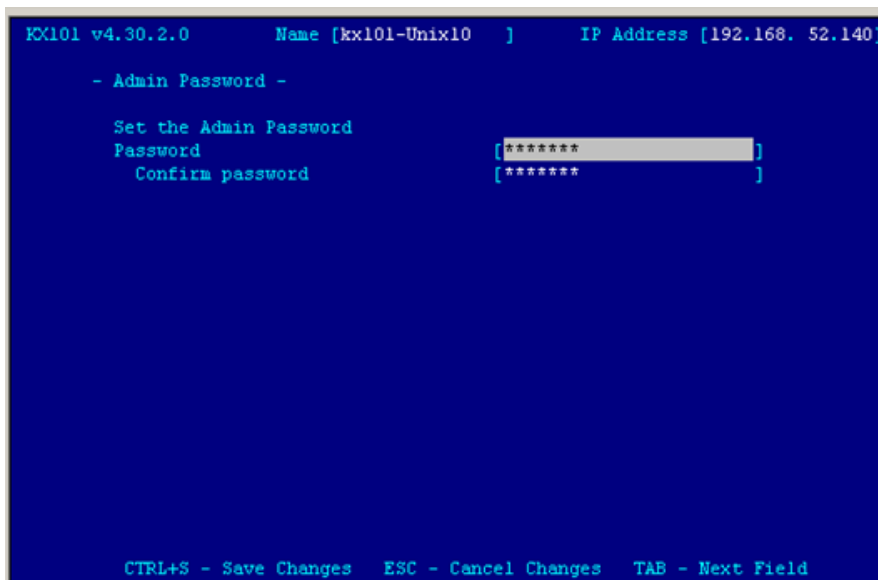


Figure 10 Admin Password Screen

## Reset to Factory Default Settings

On the Main Menu, select [F] **Reset to Factory Default Settings** to delete and personalized configuration settings or changes you have made.

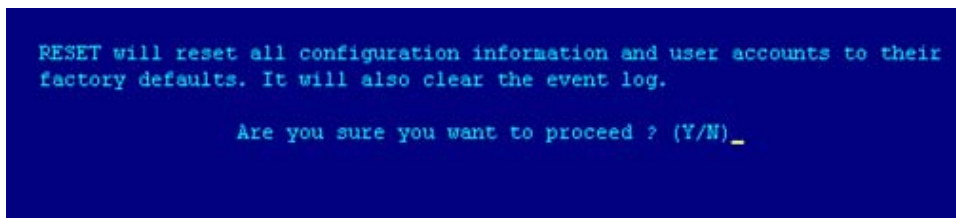


Figure 11 RESET Confirmation Screen

## Restart or Shutdown

On the Main Menu, select [R] **Restart or Shutdown the KX101** to restart or shut down the unit. Restarting will apply any changes to configuration and refresh the unit.

## Diagnostics

On the Main Menu, select **[D] Diagnostics** to view the KX101 Diagnostic functions window. The functions displayed are designed to allow Raritan's Technical Support Staff to assist you in case of troubleshooting; please do not activate these functions if you are unfamiliar with their intended use. Please note that when you close the Diagnostic screen, the KX101 unit will log out, and you must restart your session.

```
-[ KX101 Diagnostic Console ]-----[ 192.168.052.140 ]-
V          View log                LOG      Set log mask
<ENTER>   View more log            M        Insert log marker
P          Pause Log                R        Resume log
C          Clear the log
NETSTATS  Network Statistics        PING     Send a network ping
RESET     Reset to factory defaults RESTART  Restarts KX101
TRACEROUTE Print the route packets

Type HELP <commandName> to get more information.
Type X    to exit the diagnostic console.
-----
>_
```

Figure 12 KX101 Diagnostic Screen

## Administrator Password

If you lose or misplace your administrator password, recover the factory default password via the KX101's serial Admin port.

1. Type the username **admin**.
2. Type the password **R\*E\*S\*E\*T** (case-sensitive).

---

**Note:** This username and password recovery works **ONLY** from the serial Admin console.

---

When this sequence is recognized, KX101 will perform these specified reset actions as displayed in the KX Manager Security Setting panel:

- Enable local factory reset (default)
- Enable local admin password reset
- Disable all local resets





## Chapter 3: Raritan Remote Client (RRC)

Raritan Remote Client (RRC) is Dominion KX and KX101's graphical user interface, which provides remote access to the target servers connected to a KX unit. Most users invoke Internet Explorer, while other users, particularly those operating over a modem connection, choose to invoke RRC standalone. Please note that modem use is not supported with KX101.

### Invoking RRC via Web Browser

KX101 features Web Browser access capabilities, providing a connection from any Windows-based Remote PC running Microsoft Internet Explorer 6.0 (FireFox, and Safari are supported by Raritan MPC [Multi-platform Client]. Please refer to Raritan's **MPC User Guide** for additional information).

### Client PC Video and Display Drivers

---

For RRC to operate properly, it is highly recommended to load and use compatible manufacturer specific video and display drivers on the client PC instead of relying on Microsoft generic drivers.

### Security Settings

---

In order to access KX101 via web browser, your web browser must be configured appropriately, in particular, the Internet Explorer security settings tab:

- **Download Signed ActiveX controls** should be set to either "Enable" or "Prompt"
- **Run ActiveX controls and plug-ins** should be set to either "Enable" or "Prompt"

Please consult your Microsoft Internet Explorer documentation for details regarding these settings.

---

*Note: Microsoft Windows 2000, Microsoft Windows XP, and Microsoft Windows 2003 restrict certain types of users from downloading and running ActiveX controls and plug-ins, regardless of the above settings in Internet Explorer. Please consult your Microsoft Windows documentation for more information.*

---

### Launching RRC

---

1. Ensure that your browser security settings are configured appropriately and type the IP address assigned to your KX101 unit (see **Chapter 2: Installation, Initial Configuration**) in the URL/ Address text box of your web browser.

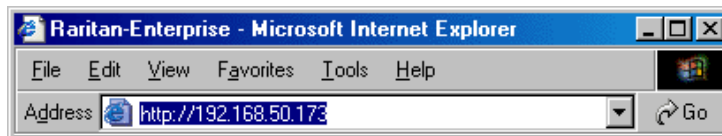


Figure 13 Type the IP Address of your Dominion KX unit

---

*Note: KX101 ships with factory DHCP default and fallback to the static IP Address of 192.168.0.192 (net mask: 255.255.255.0, Gateway 192.168.0.1).*

---

2. KX101 will redirect you to an HTTPS (128-bit) secure web page for launching RRC.

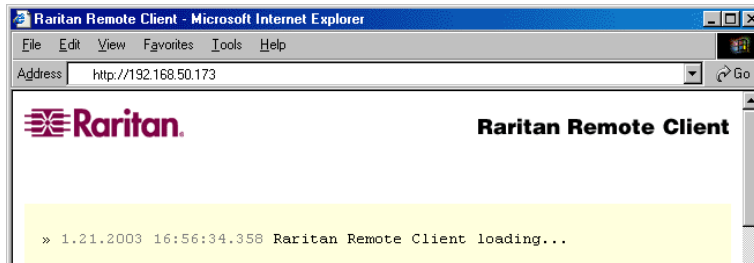


Figure 14 RRC Loading Screen

Depending on your browser's security configuration, you may see any or all of the following dialog boxes, confirming access and launch of an externally-provided program. Click **Yes** to advance through any of these prompts.

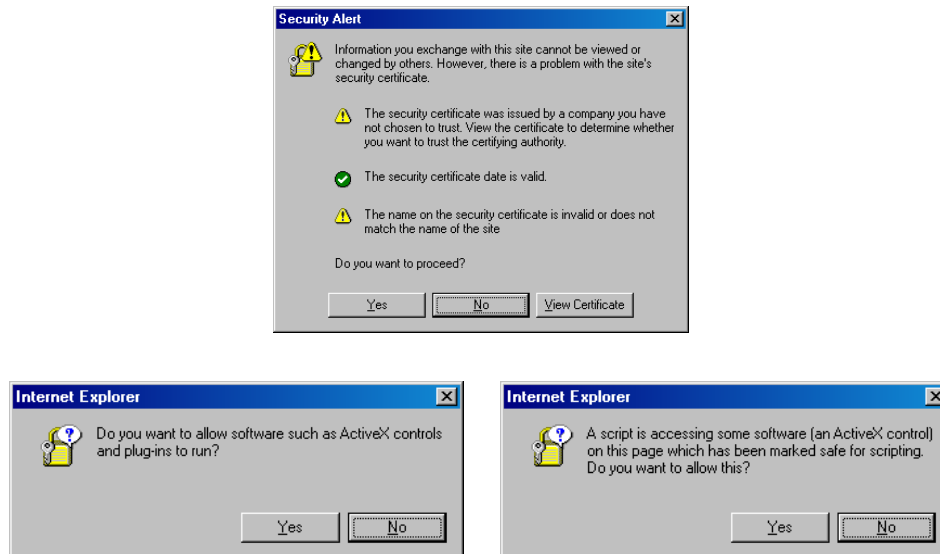


Figure 15 Possible Security Alert Screens

## Removing RRC from the Browser Cache

---

To remove RRC from your browser cache for any reason, follow the standard procedure for your Web browser software.

Directions for Internet Explorer v6.0:

1. If you have used RRC recently, exit all instances of Internet Explorer, and then restart Internet Explorer.
2. On the Internet Explorer **Tools** menu, click **Internet Options**.
3. When the **Internet Options** dialog box appears, click on the **General Settings** tab, and click **Delete Files**.
4. Click on the **Settings** tab, and then click **View Objects**.
5. Internet Explorer will display a list of cached program objects. Select any entries named "TeleControl Class," "Raritan Console," or "Power Board" and delete them.

## Raritan Multi-Platform Client (MPC)

Non-Windows users can now connect to target servers through the KX101. MPC can be run via Web browsers and standalone. Raritan MPC, depending on your browser, will launch automatically. Instructions on its use are very similar to those of RRC and follow later in this chapter, and for further instructions, please refer to Raritan's MPC User Guide.

### Optional: Installing Standalone RRC Client

---

***Note:** This step is optional. KX101 can be accessed from a Remote PC either by installing RRC software, or by launching RRC via web browser (see previous section). Accessing KX101 via web browser does not require any software installation on the Remote PC. This section lists the steps required to invoke RRC using standalone software, which may be useful for accessing Dominion KX via modem or if you wish to close firewall access to ports 80 and/or 443.*

---

1. Launch your Web browser and go to Raritan's Web site ([www.raritan.com](http://www.raritan.com)). Click **Support** in the top navigation bar, and then click **Firmware Upgrades** in the left navigation bar (or type the URL [www.http://raritan.com/support/sup\\_upgrades.aspx](http://www.raritan.com/support/sup_upgrades.aspx)).
2. Scroll down the page until you see the **Dominion KX** section.
3. Locate the appropriate version of the standalone RRC client for the KX Release you will be using.
4. The entry for the standalone RRC client is a .zip file which contains the release notes and the Installer for Standalone RRC. Check the release notes for the latest information.
5. You can download the .zip file to your client machine or simply click on the .zip file entry.
6. Double-click on the Installer executable in the .zip file and follow the on-screen instructions in the InstallShield Wizard to complete RRC installation on your Remote PC. Be sure to check the release notes for the latest information and any release specific instructions.
7. Depending upon the configuration of your PC, the RRC installation program may also automatically install DirectX and Microsoft Foundation Class libraries, if they are required. If so, you will be asked to restart your PC after installation.
8. A Raritan Remote Client icon will appear on your desktop. Click on this icon to launch the standalone RRC client.
9. The standalone client can be uninstalled in the **Add or Remove Programs** applet in the Windows **Control Panel**. You must uninstall before installing a new version of Standalone RRC.

## RRC Window Layout

RRC functions are grouped into five general sections on the screen. Each section will be discussed in detail further in this chapter.

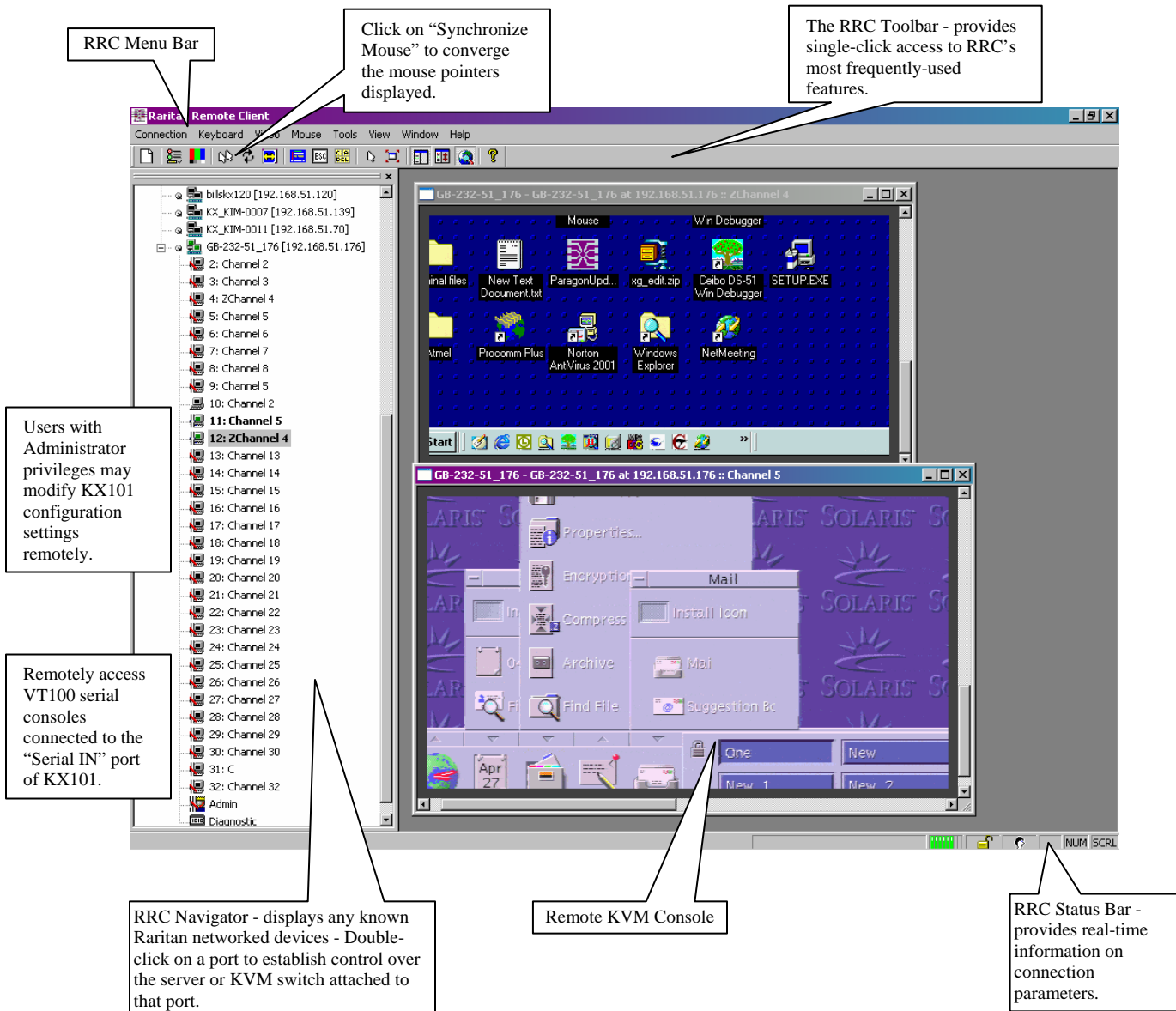


Figure 16 RRC Screen Components

## RRC Navigator

The RRC Navigator provides a tree view of every known Raritan KVM Over IP device so you can access all Raritan networked appliances for which a connection profile exists and/or all Raritan devices automatically identified on the network.

**Note:** Automatic Raritan device identification uses the UDP protocol, and will typically identify all Raritan devices on your subnet. Network administrators rarely allow UDP to function outside of a subnet. Automatic Raritan device identification will find only those Raritan devices that are configured to use the default TCP Port (5000) or other "broadcast" ports as set in the **Options** panel on the **Tools** menu.

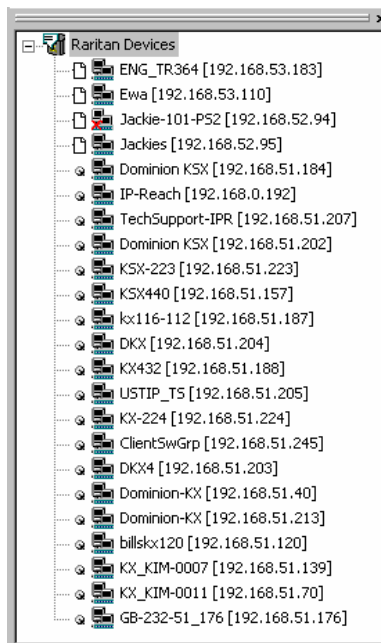





Figure 17 Expanded RRC Navigation Tree




Each device entry in the RRC Navigator provides two icons to communicate network status and connection profile information. A connection profile is generally created by an RRC user in order to store personalized information about specific devices (please see next section **Creating New Profiles** for additional information).

Profiled Devices will be identified in the RRC navigator by the Description field in the profile. Automatically-identified devices will be named according to the **Manager Name** field in KX Manager's **Network Configuration** screen (please see **Chapter 4: Administrative Functions, Network Configuration** for additional information).

#### **Left Icon (Connection Profile)**

	Profiled – A network connection profile exists for this device.
	Modem Profile – A modem connection profile exists for this device.
	Not Profiled – RRC found this device on the network, but a connection profile does not exist for it.





**Right Icon (Network Status)**

	Connected (green) – You are currently authenticated and connected to this device.
	Available (black) – This device is currently available on the network, but you are not currently connected to it.
	Unavailable – A profile exists for this device, but it is not currently available on the network. (Note that all devices with modem profiles to which you are not currently connected will display this icon.)

For each Raritan device to which you are connected, RRC Navigator expands its display tree to show each port for which you have access.




- Ports displayed with a green icon indicate that you are connected to that port.
- Bold type indicates which port is currently displayed (active) in the remote desktop area of the client.

For each server port entry, RRC navigator displays the following icons:

	Connected (green)
	Available for connection
	Unavailable (no device connected, or access is blocked)
	Unavailable (in use by another)

**Navigator Options**

Certain RRC Navigator attributes may be customized to your preferences.

	Display / Hide Navigator – Toggle whether the RRC Navigator is shown. This option can also be toggled by choosing <b>View → Navigator</b> from the Menu Bar.
	Refresh Navigator – Update the device status information shown in the RRC Navigator.
	Show Browsed Devices – Toggle whether RRC Navigator should display “Not Profiled” devices automatically found on the network or show only devices for which profiles exist. This option can also be toggled by choosing <b>View → All Devices</b> from the Menu Bar.

*Note: The Browse connection method is the only method of connecting to a Raritan Device configured to use DHCP IP addressing.*

## RRC Navigator – Display and Sorting Options

---

### Showing Ports

In RRC, you can select which ports to view in the Navigation panel by selecting **Show** options on the **View** menu.

- **All:** shows or hides non-profiled devices from the navigator view
- **Unassigned Channels:** shows or hides channels with targets
- **Tools:** shows or hides the Admin and Diagnostic ports

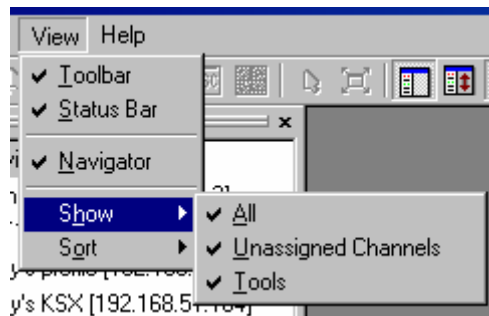


Figure 18 View → Show Menu Options

## Sorting Ports

Use the **Sort** options on the **View** menu to organize KX port information; sort ports by channel number, channel name, or channel status.

### Sort by Channel Number

When sorted by channel, ports are listed numerically.

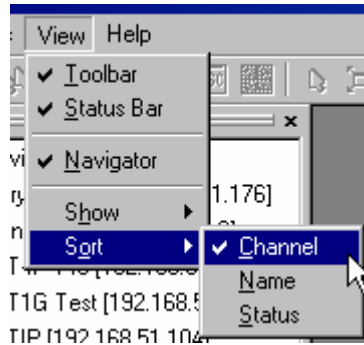


Figure 19 Sort Ports by Channel

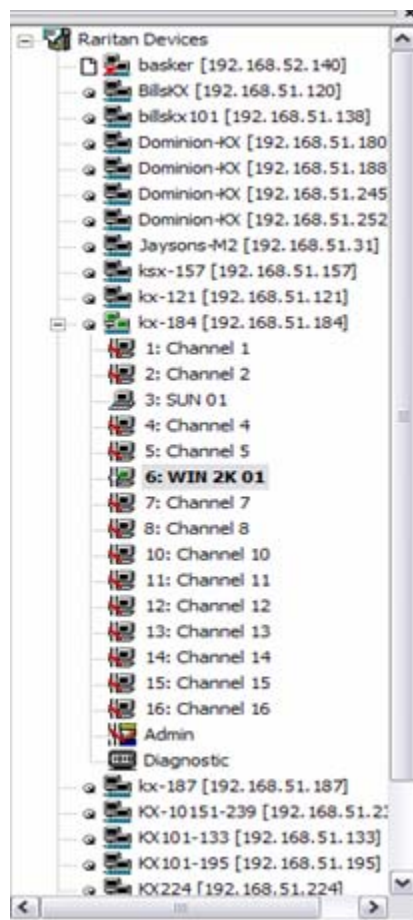


Figure 20 Navigator Displaying Ports in Channel Order



## Sort by Name

When sorted by name, port names are sorted alphanumerically within each group.

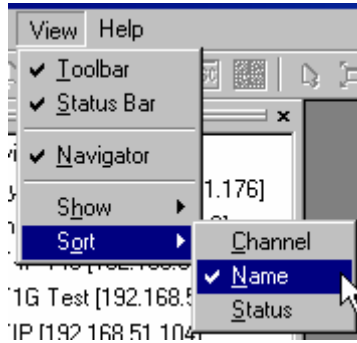


Figure 21 Sort Ports by Name

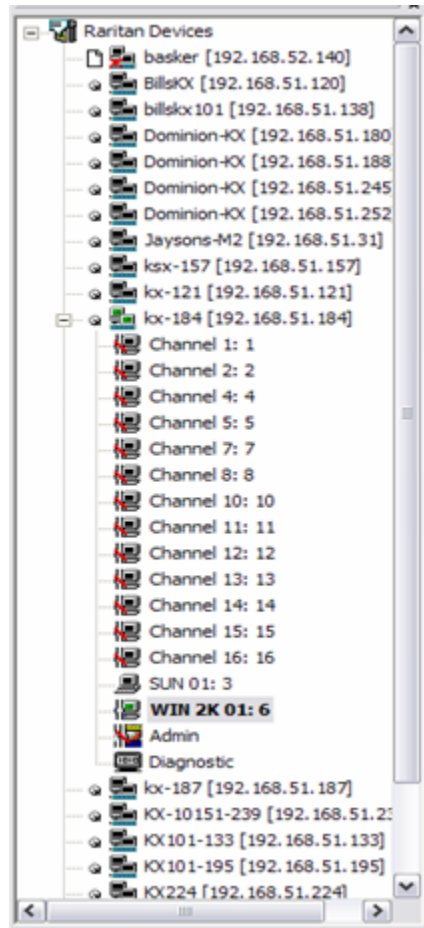


Figure 22 Navigator Displaying Ports in Name Order

## Sort by Status

Ports are sorted in the following order:

- Active Channels
- Busy Channels
- Available Devices
- Unavailable Devices

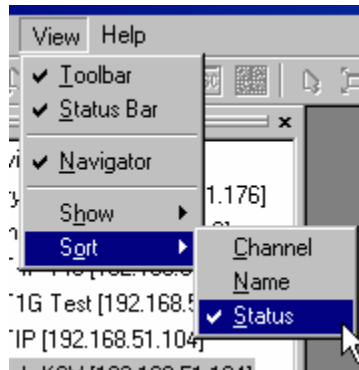


Figure 23 Sort Ports by Status

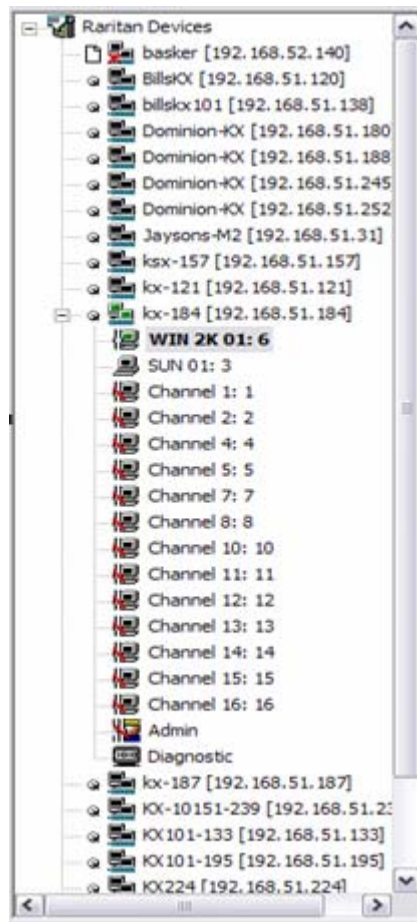


Figure 24 Navigator Displaying Ports in Status Order

## Creating New Profiles

Create a connection profile to store important information about your Raritan device, such as IP Address, custom TCP ports, preferred compression settings, and custom security keys. A profile is required to access devices outside your subnet, and for devices accessed via dial-up connection. Individual users can create individual personal profiles, that is, profiles are not shared amongst multiple users. The profile enables each user to set up a personalized connection.

*Note: If your Raritan device is configured to use a custom TCP port (see Chapter 4: Administrative Functions, Network Configuration), or a group security key (see Chapter 4: Administrative Functions, System-Level Security Parameters), first create a connection profile so you can access the device.*

1. There are two ways to create a profile. For devices automatically discovered, right-click on the device name in the RRC Navigator and select **Add Profile** from the shortcut menu. For other devices, on the **Connection** menu, click **New Profile**. The **Add Connection** dialog appears. Options are grouped into three tabs.

### A. Connect tab

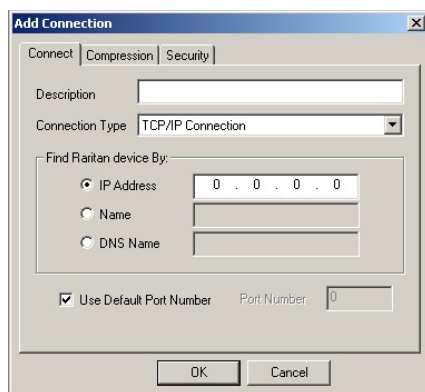


Figure 25 Connect tab

- **Description:** Type a text name that identifies the Raritan device you are configuring, such as “Atlanta\_Datacenter.” This name will identify the device in the RRC Navigator.
- **Connection Type:** Select TCP/IP Connection for a LAN/WAN connection, or select Dial-Up Connection for a direct analog modem connection to the Raritan device.

For a **TCP/IP Connection**, select the option button before the method by which RRC should locate your Raritan device:

- **IP Address:** Type the IP address assigned to your Raritan device (see **Chapter 4: Administrative Functions, Network Configuration**).
- **Name:** Type the name assigned to your Raritan device during initial setup (see **Chapter 4: Administrative Functions, Network Configuration**).
- **DNS Name:** If you have configured your DNS server to resolve a DNS name to the IP address that you have assigned to your Raritan device, type the DNS name. Please note that you cannot set a DNS address on the KX101.

*Note: Dial-Up Connection properties apply only to the Dominion KX unit, not KX101.*

For a **Dial-Up Connection**, enter the dialing parameters that RRC should use to establish a connection:

- **Phone Number:** Be sure to include any additional codes that RRC should dial to establish a connection, such as country codes, area codes, or outside line access codes.

- **Modem:** Select the modem, as configured in Windows, which RRC should use to dial and connect to your Raritan device.

Select a TCP Port to use:

- **Use Default Port Number:** KX101 is configured by default to use TCP Port 5000 for communicating with RRC. The KX101 unit can be configured to use a different TCP Port (see **Chapter 4: Administrative Functions, Network Configuration**); if so, uncheck the **Use Default Port Number** option, and enter the configured TCP Port to be used.

## B. Compression tab

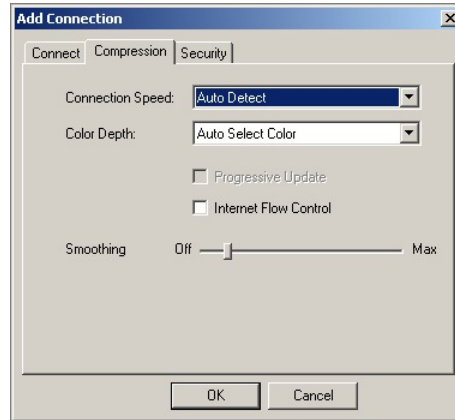


Figure 26 Compression Tab

Settings under the **Compression** tab are adjustable via the RRC client, and not necessary for pre-configuration in the Connection Profile. If you wish to pre-configure these settings, however, please refer to the section **Connection and Video Properties** in this chapter.

## C. Security tab

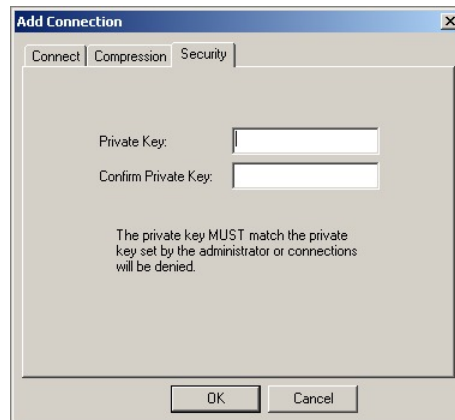


Figure 27 Security tab

If you have configured your KX101 unit to use a private security key (see **Chapter 4: Administrative Functions, System-Level Security Parameters**), enter it here in order to be authorized to initiate a connection with that Dominion KX unit. Click **OK** when you have completed the fields. When you have completed the **Connect** and **Security** tab screens, click **OK** create the connection.

## Modifying Profiles

---

To modify a profile in RRC, select the device in the RRC Navigator and right-click on it. Select **Modify Profile** from the shortcut menu. When modifying a device profile, please note that the profile description and the IP Address of the device **cannot** be changed.

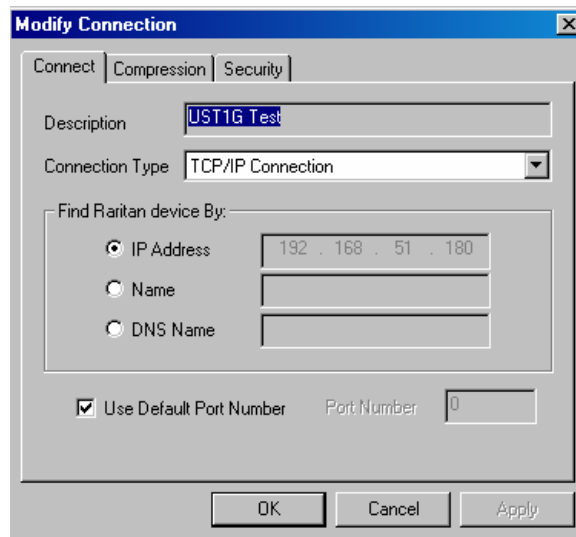


Figure 28 Modify Connection screen

## Deleting Profiles

---

To delete a profile in RRC, select the device in the RRC Navigator and right-click on it. Select **Delete Profile** from the shortcut menu. When RRC asks you to confirm deletion, click **Yes** to delete the profile for this device, or click **No** to return to RRC without deleting.

## Establishing a New Connection

---

After typing your user name and password, double-click the icon of a Raritan networked device in the RRC Navigator to connect. You can also right-click on the device name and select **New Connection** from the shortcut menu.

***Note:** The default KX101 login user name is **admin**, with the password **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 username password as soon as possible.*

If you do not see an icon for your KX101 in the RRC Navigator, please follow the instructions in the **Creating New Profiles** section in this chapter to create a new connection profile for your KX101 unit.

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

- **Username / Password:** Raritan usernames and passwords are case-sensitive.
- **TCP Port:** If you have configured your Raritan Device to use a non-default TCP Port, this information must be entered into its connection profile.
- **Firewall Settings:** If you are accessing a Raritan Device through a firewall, that firewall must be configured to allow two-way communication on TCP Port 5000 (or the custom TCP Port to which your Raritan Device has been configured).
- **Security Key:** If you have configured your Raritan Device to require a group security key, that key must be entered into the device's connection profile.

## Closing a Remote Connection
















To end your KX101 connection, right-click on the icon, and select **Disconnect** from the menu.

## RRC Toolbar and Shortcuts

The RRC Toolbar provides one-click access to the most frequently-used commands.



Figure 29 RRC Toolbar

BUTTON	BUTTON NAME	FUNCTION
	New Profile	Creates a new Navigator entry for a Raritan device; same results as selecting <b>Connection</b> → <b>New Profile</b> in the menu bar.
	Connection Properties	Opens Modify Connection Properties dialog box to manually adjust bandwidth-correlated options (Connection Speed, Color Depth, etc.).
	Video Settings	Opens the Video Settings dialog box to manually adjust video conversion parameters.
	Synchronize Mouse	In dual-mouse mode, forces realignment of target server mouse pointer with Raritan Remote Client mouse pointer.
	Refresh Screen	Forces refresh of video screen.
	Auto-sense Video Settings	Forces refresh of video settings (resolution, refresh rate).
	Enter On-Screen Menu	Not applicable for KX101. Used by RRC with other Raritan products.
	Exit On-Screen Menu	Not applicable for KX101. Used by RRC with other Raritan products (on keyboard, press <b>ESC</b> key)
	Send Ctrl+Alt+Del	Sends a Ctrl+Alt+Del key sequence to the target server.
	Single Cursor Mode	Enters Single Cursor Mode, in which the local PC's mouse pointer no longer appears on-screen. Press <Ctrl+Alt+X> to exit this mode.
	Full Screen Mode	Maximizes the screen real estate to view the target server desktop.
	Show / Hide Navigator	Toggles whether or not the RRC Navigator is displayed.
	Refresh Navigator	Forces a refresh of the data displayed by the RRC Navigator.
	Show / Hide "Browsed" Devices	Toggles whether or not the RRC Navigator displays Raritan Devices automatically identified on the network (that do not have pre-configured profiles associated with them).
	About	Displays version information about Raritan Remote Client.

## RRC Status Bar

The RRC Status Bar displays session information about your connection to your KX101.

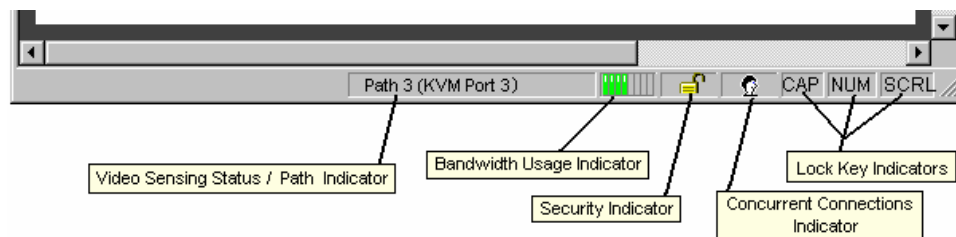


Figure 30 RRC Status Bar Components

- **Video Sensing Status / Path Indicator:** indicates the occurrence of video sensing, during connections to target KVM Server ports.
- **Bandwidth Usage Indicator:** indicates how much of your total available bandwidth is currently being used. The **Connection Speed** setting, found under the Compression tab of the Connection Properties screen, determines total available bandwidth.
- **Security Indicator:** indicates whether the current remote connection is protected by encryption. Encryption requirements are set during Dominion KX configuration (see **Chapter 4**). When a KX101 device is configured for **No encryption** or **SSL Authentication, NO data encryption**, the Security Indicator is represented on the Status Bar as an open lock. When **SSL authentication, data encryption** or **SSL authentication, SSL encryption** is selected, the Security Indicator is represented on the Status Bar as a closed lock.
- **Concurrent Connections Indicator:** indicates if multiple remote users are currently connected to the same Dominion KX target server, showing one icon for a single connected user, and two icons if two or more users are connected. Concurrent connection ability can be set globally under **PC Share Mode** on the Security Configuration screen (see **Chapter 4**), or set per individual user in the **Concurrent Access Mode** setting on the User Account Settings screen (see **Chapter 4**).
- **Lock Key Indicators:** indicates the status of the current target KVM Server, with respect to the activation of the Caps-Lock, Num-Lock, and Scroll-Lock keys. If these keys are enabled on the target server being viewed, this affirmative status will be reflected on the Status Bar as indicated.

## Keyboard Shortcut Menu

To access RRC's keyboard shortcut menu, press **CTRL+ALT+M**. Execute any of the commands on the shortcut menu either by pressing the underscored letter on the button face, or by clicking the command button in the menu itself.



Figure 31 RRC Keyboard Shortcut Menu

### Keyboard Execution:

To:	PRESS CTRL+ALT+M, AND THEN PRESS:
Toggle to/from Full/Normal Screen Mode	F
Perform video Auto Sensing*	A
Display connection information*	I
Display or Set connection properties*	P
Display or Set Video Settings*	V
Refresh screen	R
Synchronize mouse	Y
Change to/from Single/Double cursor mode	S
Send CTRL+ALT+DEL to the target system	D
Send CTRL+ALT+M to the target system	N
Exit the Dialog/Menu without altering the keyboard state	Esc

\* If Full Screen Mode is active, executing this command will automatically end Full Screen Mode.



## Remote KVM Console Control

Once you establish a connection with a KX101 unit, that unit's icon in the RRC Navigator expands to display all ports enabled for remote access.

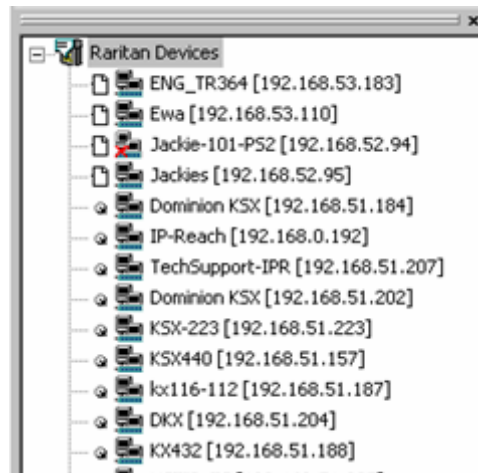


Figure 32 Navigation Tree

There are a few ways to establish a remote KVM console connection:

- Double-click on the KVM port you want to control
- Right-click on the port and select **Switch** from the shortcut menu
- Right-click on the port and select **New Connection** from the shortcut menu.

Selecting the first or second option above closes any previous connection before connecting to the new port, while selecting the third option allows you to connect to the selected port without closing any previous connections, creating a new connection if the device supports multiple concurrent connections (KX2 and KX4 devices allow multiple concurrent connections).

Once connected, the KX101 displays real-time video output by the target server that is connected to your Dominion KX KVM port. This video is compressed and encrypted according to the configuration settings specified by the Administrator (please see **Chapter 4**). You now have complete, low-level control of the KVM console as if you were physically connected to the server. To close a connection, on the **Connection** menu, click **Close**, or right-click on the KVM port and click **Disconnect** on the shortcut menu that appears.

## Single Mouse Mode / Dual Mouse Mode

When remotely viewing a target server that uses a pointing device, you will see two mouse pointers in the Remote Desktop. When your mouse pointer lies within the Remote Desktop area of RRC, mouse movements and clicks are directly transmitted to the target server connected. RRC's mouse pointer, generated by the operating system on which RRC is running, slightly leads the target server's mouse pointer during movement, a necessary result of digital delay.

On fast LAN connections, you may want to disable the RRC mouse pointer and view only the target server's pointer. To toggle between these two modes, use the **Ctrl+Alt+M** hotkey to activate the on-screen menu and press **S** to select **Single/Double Cursor** (or you can click the **Single Mouse Pointer** mode icon in the RRC toolbar).

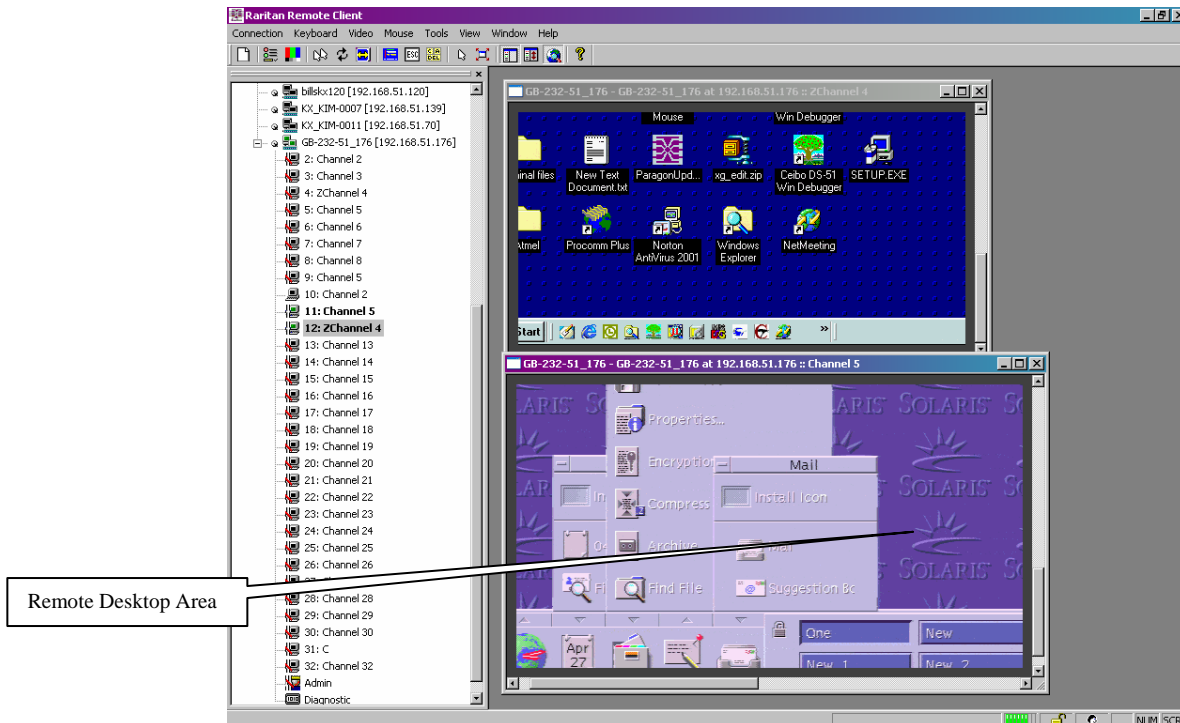


Figure 33 Remote Desktop, where dual mouse cursors will appear

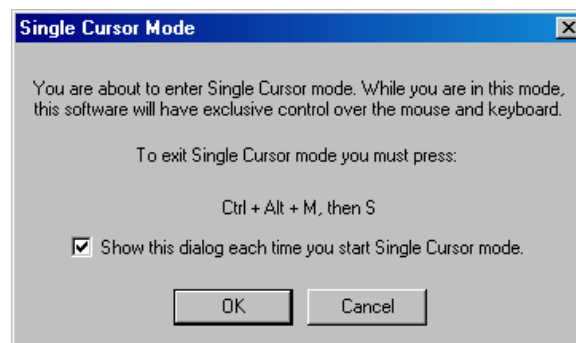


Figure 34 Single Cursor Mode Confirmation Window

For better alignment of mouse pointers, simultaneously press the keys **Ctrl+Alt+M** to view the shortcut menu and use the **Synchronize Mouse** shortcut. This forces the realignment of the mouse pointers. If you have carefully followed **Chapter 2: Installation, Configuring Target Servers** and the mouse pointers remain out of sync, click on the **Auto-Sense Video** button on the RRC Toolbar.

---

## Automatic Mouse Synchronization

---

When in **Dual Cursor** mode, the system will automatically align the mouse pointers when the cursor is inactive for 15 seconds. Enable this feature by selecting **Options** from the **Tools** menu and clicking on the checkbox before **Auto-Sync mouse in two-cursor mode**.

---

## Mouse Mode

---

You can select the mouse mode from RRC's **Mouse** menu. There are three possible choices:

- **Standard:** This mode requires that acceleration be disabled, and is the standard mouse mode. With Standard mode, the mouse parameters must be set to specific values as described in **Chapter 2: Installation**.
- **Intelligent:** This mode uses an advanced algorithm to predict the mouse acceleration based on test behavior. Setting this mode commences a mouse synchronization that moves the target mouse at various speeds, and then uses this information to predict what acceleration speed is used on the target system. With Intelligent Mouse Mode, for most servers, the mouse parameters need not be changed on the target server. For Windows targets, Active Desktop must be disabled to use Intelligent Mouse.
- **Absolute:** This is the best choice and performs exact mouse synchronization with the target system. Target mouse acceleration is permitted, so any mouse setting on the target may be used. This requires a USB target system, and is only currently available with Raritan's KX101.

## Intelligent Mouse Mode Settings

Please note that there are certain settings required that allow Intelligent Mouse Synchronization to function properly:

1. Active desktop must be disabled on the target.
2. The upper left corner of the screen cannot contain a window or an animated background.
3. The cursor you are using cannot be animated.
4. "Enhanced pointer precision" or similar mouse properties should not be enabled.
5. After auto-sensing, if the window is not perfectly centered (that is, there's black banding on the borders of the screen), Intelligent Mouse Synchronization will not work perfectly, and in extreme cases, will not work at all.
6. When the resolution of the target changes, you must re-synchronize the mouse.
7. You must choose "Best Possible Video mode" in the Video Settings window (see **Video Settings**, later in this chapter) in RRC and force auto sense (using the RRC button).
8. You must disable all extra mouse features such as "snap mouse to default button in dialog boxes" and similar.
9. On a Linux- or Unix-based target, do not set point acceleration variables.

Please note that the mouse algorithm might not work for very slow or very high speed values. In addition, it may sometimes take slightly longer than five seconds to synchronize the mouse.

If Intelligent Mouse Synchronization fails, the mouse will revert to standard behavior without changing the mode itself from intelligent to standard.

## Full Screen Mode

**Full Screen** mode removes the surrounding RRC graphical interface and your local desktop area, filling your monitor with the video from the target server. Your monitor's resolution will be adjusted to match the resolution of the target server, if your graphics system supports it.

To view the video resolutions your system supports, access **Control Panel**, double-click **Display**, and click on the **Settings** tab.

To enter **Full Screen** Mode once connected to a target, from the **View** menu, click **Full Screen**, or press the keys **Ctrl+Alt+M**, and then **F** to select **Full/Normal Screen**. If your graphic system does not support the resolution of the target system, you will be unable to enter Full Screen mode and will see a message warning that your resolutions should be changed to execute the command.

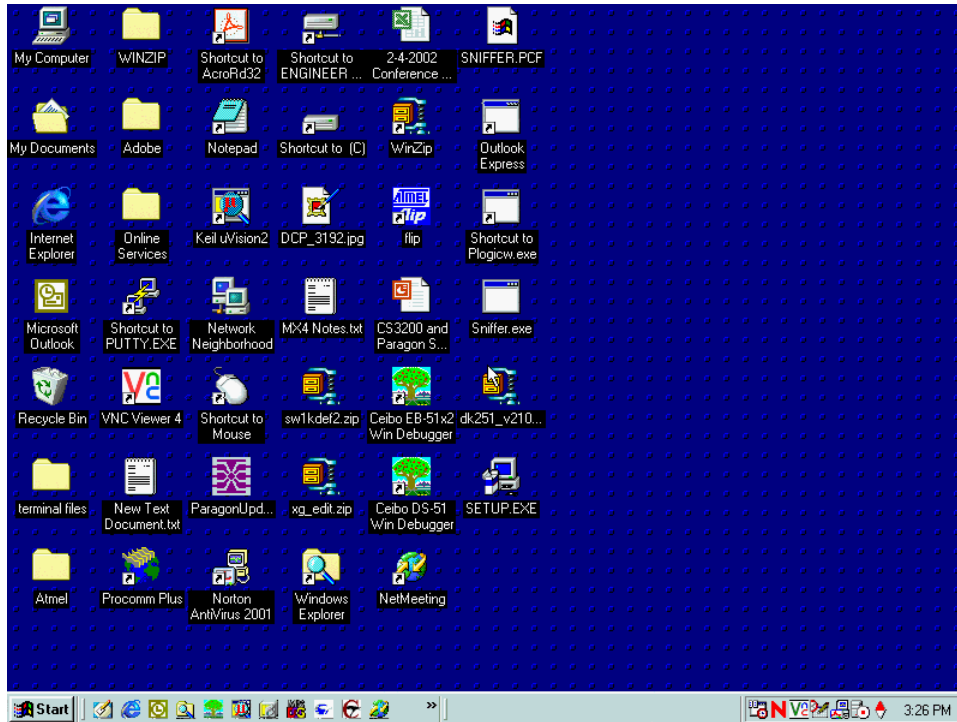


Figure 35 Full Screen Mode View

## Scaling

Scaling your target window size allows you to view the entire contents of the target server window without using the scroll bar. This feature increases or reduces the size of the target video to fit the RRC window size, so that you see the entire target server desktop while maintaining the full standard RRC view.

To activate **Scale Video** mode, on the **View** menu, click **Scale**. To exit this mode, on the **View** menu, click **Scale**.

## Auto-Scroll

The auto-scroll feature automatically scrolls the video display in the direction of the cursor, when the cursor approaches the edge of the display. A thin border can be optionally displayed around the perimeter of the remote server screen via an option on the **Tools** menu.

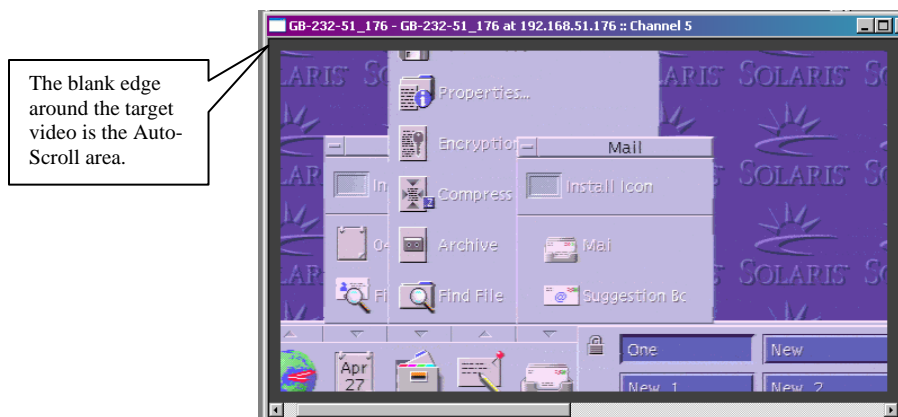


Figure 36 Auto-Scroll Border

## Keyboard Handler

RRC sends all keystroke combinations to the target system with the following exceptions:

- **CTRL+ALT+DEL** – Operates as usual, the sequence is sent to the local system and the Windows Security (Task Manager, Shutdown, etc.) dialog is displayed.
- **CTRL+NUM LOCK** – This toggles the state of the NUM LOCK LED if the NUM LOCK state of the local system disagrees with that on the target system.
- **CTRL+CAPS LOCK** – This toggles the state of the CAPS LOCK LED if CAPS LOCK state of the local system disagrees with that on the target system.
- **CTRL+SCROLL LOCK** – This toggles the state of the SCROLL LOCK LED if SCROLL LOCK state of the local system disagrees with that on the target system.
- **CTRL+ALT+M** – Brings up a dialog/menu providing normal RRC shortcuts (described below).
- Keystrokes used when generating user-defined keyboard macros.
- **Print Scrn** – Treated locally and copies the screen to the clipboard.


There are no other exceptions. For example, **ALT+F4** closes the current program on the target system.

## Keyboard Macros

KX101's Keyboard Macro feature ensures 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 RRC is running.

### Ctrl+Alt+Delete Macro

Due to its frequent use, a Ctrl+Alt+Delete macro has been pre-programmed into RRC.

	Send Ctrl+Alt+Del	Sends a Ctrl+Alt+Delete macro to the target server.
---	----------------------	---

Clicking on the **Ctrl+Alt+Delete** shortcut in the RRC Toolbar sends this key sequence to the server or KVM switch to which you are currently connected. In contrast, if you were to physically press the **Ctrl+Alt+Delete** keys while using RRC, the command would first be intercepted by your own PC due to the structure of the Windows operating system, instead of sending the key sequence to the target server as intended.

### Building a Keyboard Macro

These directions describe how to create a keyboard macro for the Windows command **Minimize All Windows/Show Desktop**. Follow these steps, substituting the appropriate key combination for the command you want, to create your own macro.

*For example:* In Windows, pressing a keyboard macro is a shortcut that sends a command to your PC. When connected to a target server with RRC, a keyboard macro is one means to accomplish this task on the target server – because pressing the key combination results in your own client PC intercepting the command and performing it – instead of sending the command to the target server as intended.

1. On the **Keyboard** menu, click **Keyboard Macros**.
2. When the **Keyboard Macros** window appears, click **Add** to add a new macro. The **Add Keyboard Macro** window appears.

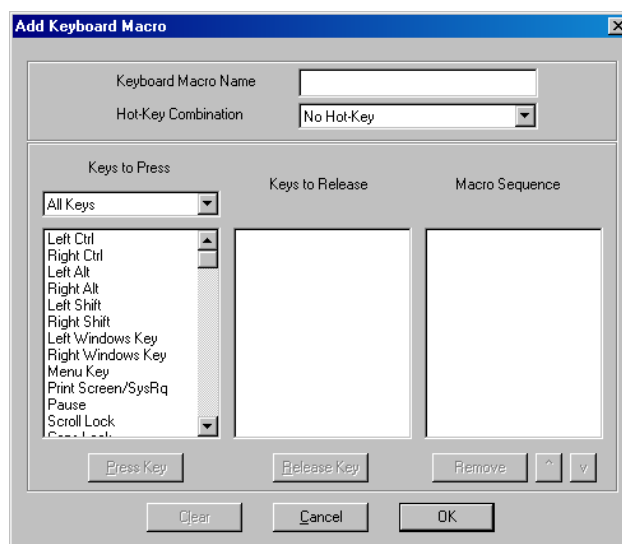


Figure 37 Add Keyboard Macro Window

3. Build the Keyboard Macro by editing the fields in the **Add Keyboard Macro** window:

- Type a name in the **Keyboard Macro Name** field. This name will appear on the RRC Menu Bar after the macro is created. In this example, type **Minimize All Windows**.
- **Optional:** In the **Hot-Key Combination** field, type a keyboard combination. This allows you to execute the macro from your keyboard when RRC is running. *In this example,* press the **Ctrl, Alt** and number **1** keys (**Ctrl+Alt+1**).
- In the **Keys to Press** drop-down list, select each key for which you would like to emulate key presses – in the order by which they are to be pressed. Click **Press Key** after each selection. As each key is selected, it will appear in the **Keys to Release** field. *In this example,* select two keys: the **Windows** key and the letter **D** key.
- In the **Keys to Release** field, select each key for which you would like to emulate key releases – in the order by which they are to be released. Click **Release Key** after each selection. *In this example,* both keys pressed must also be released.
- Review the **Macro Sequence** field – the contents are automatically generated depending on the **Keys to Press** and **Keys to Release** selections. Ensure that the contents list the exact key sequence you want. To remove a step in the sequence, select it, and click **Remove**. To change the order of steps in the sequence, select the step and click **↑** and **↓** to re-order the steps.

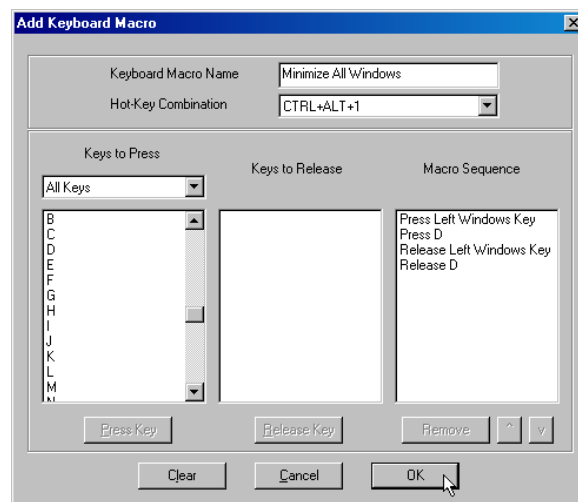


Figure 38 Add Keyboard Macro Window

4. Click **OK** to save the macro, or **Cancel** to close the window without saving. Click **Clear** to clear all field and start over. When you click **OK**, the **Keyboard Macros** window appears, listing the new keyboard macro.

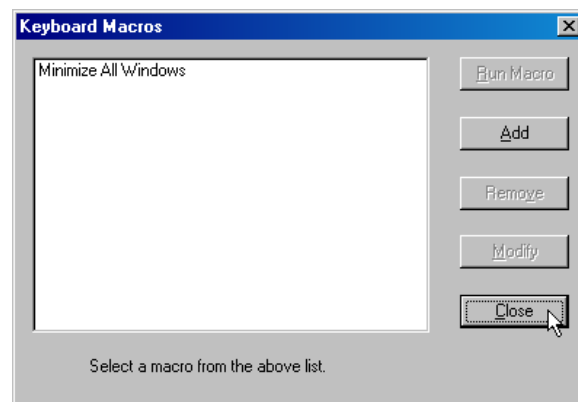


Figure 39 Keyboard Macros Window

5. Click **Close** to close the window.

## Running a Keyboard Macro

Once you have created a keyboard macro, execute it from the RRC Menu Bar, or by using the hotkey (keyboard) combination if you assigned one while creating the macro.

### Menu Bar Activation

When you create a macro, it appears under the **Keyboard** menu. From the **Keyboard** menu, click on the name of your keyboard macro.

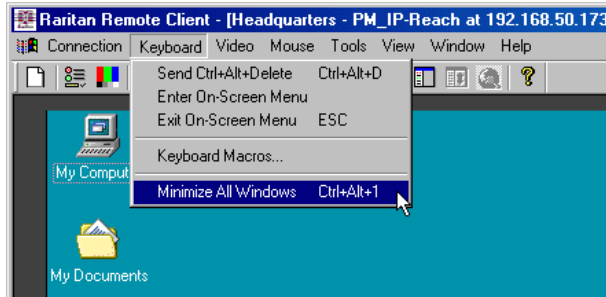


Figure 40 Minimize All Window Menu Option

### Hot-Key Activation

When you create a macro, execute it in RRC by pressing the hotkey you assigned to it. *In this example*, press the keys **Ctrl+Alt+1** simultaneously to send the Minimize All Windows combination **Windows+D** to the target server.




## Connection and Video Properties

KX101's dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. KX101 is unique in that it optimizes its KVM output for not only LAN utilization, but also via the WAN and dial-up. It also adjusts color depth and can limit video output, offering an optimal balance between video quality and system responsiveness in any bandwidth constraint.

Power users of RRC should understand the following adjustable parameters in the **Connection Properties** and **Video Settings** dialog boxes, and familiarize themselves with the effects of each setting – in different operating environments, they can be optimized to your requirements.

### Connection Properties

	<b>Connection Properties</b>	Opens Modify Connection Properties dialog box to manually adjust bandwidth-correlated options (Connection Speed, Color Depth, etc.).
---	------------------------------	--

1. On the Connection menu, click Connection Properties. The Modify Connection window appears.

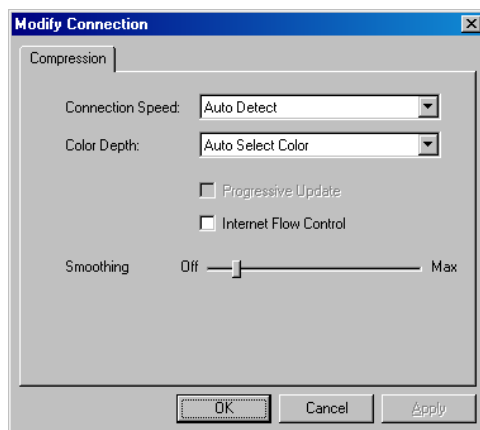


Figure 41 Modify Connection Window

- **Connection Speed:** Use the **Connection Speed** setting to manually tell KX101 of bandwidth constraints. KX101 can adapt its speed and not use more than the bandwidth that is available. KX101 detects available bandwidth automatically, but you can adjust this use.
- **Color Depth:** KX101 can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidth constraints.
  - **Progressive Update** option: Progressive Update can increase usability in constrained bandwidth environments. When **Progressive Update** is enabled, Dominion KX first sends an image of the remote desktop at lower color depths, and then provides higher color depth images as bandwidth allows.

---


Important: For most administrative tasks (server monitoring, reconfiguring, etc.), server administrators do not require the full 24-bit or 32-bit color spectrum made available by most modern video graphics cards. Attempting to transmit such high color depths, then, would waste an enormous amount of precious network bandwidth.

---

**Note:** When Color Depth is set to **Auto Select Color** (default), **Progressive Update** is automated. KX101 will enable/disable Progressive Update as needed, disabling it for fast connections and enabling it for slow connections.

- **Internet Flow Control:** When using KX101 over an unpredictable public WAN (particularly in international scenarios), checking the **Internet Flow Control** check box ensures that packets transmitted by the KX unit are received and reconstructed by RRC in the correct order.
  - **Smoothing:** The video **Smoothing** level you set instructs the KX unit to what degree color gradation shifts are relevant for transmission. Video pixels that stray from the majority color are assigned approximated color values to reduce bandwidth used and video noise transmitted. Overly high smoothing levels can result in color inaccuracies; whereas lower smoothing levels require greater bandwidth and processing power.
2. Click **OK** to set Connection Properties or **Cancel** to close the window without saving changes.

## Video Settings

	Video Settings	Opens the Video Settings dialog box to manually adjust video conversion parameters.
---	----------------	---

3. On the **Video** menu, click **Video Settings**. The **Settings** window appears.

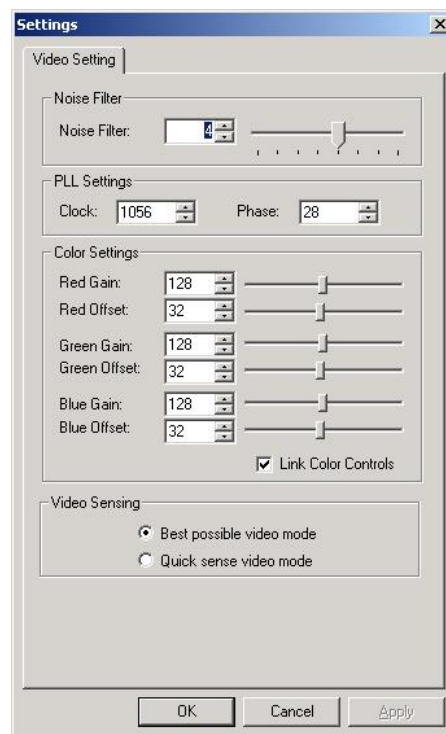


Figure 42 Settings Window

Most settings here are refreshed by performing a Color Calibration (described in the next section), or by manually forcing the KX unit to auto-detect the video settings (on the **Video** menu, click **Auto-sense Video Settings**). However, it is useful to understand the settings.

- **Noise Filter:** The KX unit can filter out electrical interference of video output from graphics cards. This feature optimizes picture quality and reduced used bandwidth.

- *Higher:* Noise Filter settings instruct KX101 to transmit a variant pixel of video only if a large color variation exists in comparison to its neighbors. However, setting the threshold too high can result in the unintentional filtering of desired screen changes.
- *Lower:* Noise Filter settings instruct the KX unit to transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.

---

*Note: Lower Noise Filter settings (approximately 1 to 4) are recommended. Although higher settings will stop the needless transmission of false color variations, true and intentional small changes to a video image may not be transmitted.*

---

- **Analog-to-Digital Settings:** The following parameters are best left to the KX unit to automatically detect (on the RRC Menu Bar, select **Video > Auto-sense Video Settings**), but a brief description of each is included here.
  - **PLL Settings:** If the video image looks extremely blurry or unfocused, the PLL Settings for clock and phase can be adjusted until a better image appears on the active target server.
    - **Clock:** Horizontal sync divider to produce pixel 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.
    - **Phase:** Phase values range from 0 to 31 and will wrap around. Stop at the phase value that results in the best video image for the active target server.
  - **Color Settings:** Gain control can be thought of as contrast adjustment. Offset control can be thought of as brightness adjustment.
    - **Red Gain:** Controls the amplification of the red signal.
    - **Red Offset:** Controls the bias of the red signal.
    - **Green Gain:** Controls the amplification of the green signal.
    - **Green Offset:** Controls the bias of the green signal.
    - **Blue Gain:** Controls the amplification of the blue signal.
    - **Blue Offset:** Controls the bias of the blue signal.
    - **Link Color Controls:** Makes all the gain slide adjusters move in unison when any one color's gain slide is moved and all the offset slide adjusters move in unison when any one color's offset slide is moved.
  - **Best Possible Video Mode:** KX101 will perform the full Auto Sense process when switching targets or target resolutions. Selecting this radio button will cause the KX unit to calibrate the video for the best image quality.
  - **Quick Sense Video Mode:** Selecting this radio button will cause the KX unit to use a quick video auto sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.
4. Click **OK** to set Video Settings or [**Cancel**] to close the window without saving changes.

---

*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.*

---

## Color Calibration

Automatic Color Calibration adjusts the color settings on the KX unit to reduce excess color noise and data during digitization of video images, increasing the performance of the KX unit. Use the Color Calibration command if the color levels (hue, brightness, saturation) of transmitted video images do not seem accurate. KX unit color settings remain the same when switching from one target KVM Server to another, so you can perform Color Calibration once to affect all connected target servers.

1. Open a remote KVM connection to any server running a graphical user interface.
2. Ensure that a solid white color covers approximately 15% or more of the target server's desktop (suggestion: open Microsoft Notepad and maximize the window).

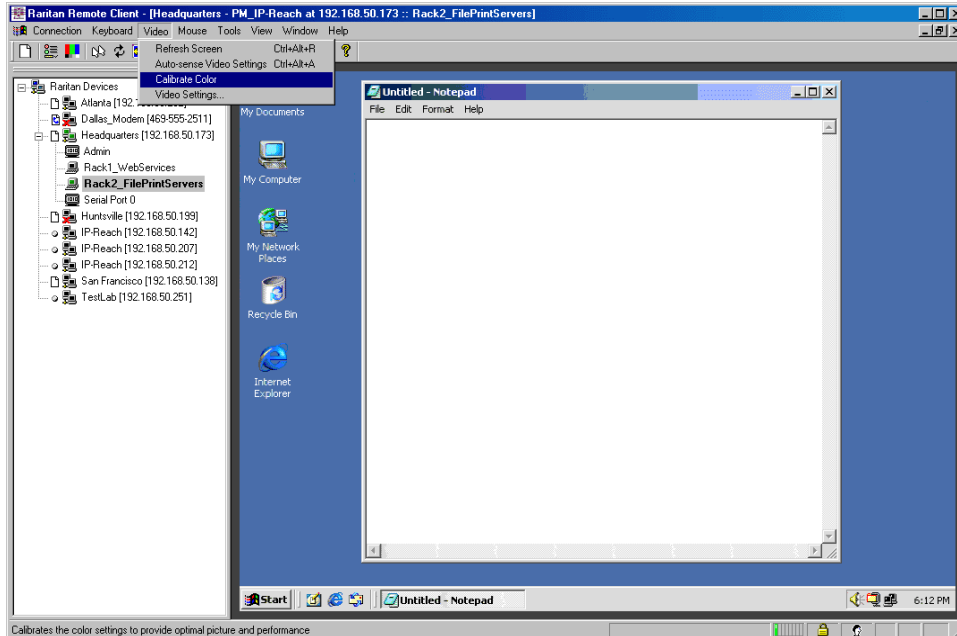


Figure 43 Example of Sizing the Notepad Window

3. On the **Video** menu, click **Calibrate Color**.

## Select Administrative Functions via RRC

Although the KX unit provides a remote interface to administrative functions through KX Manager, RRC provides an interface to frequently-used administrative functions directly from the RRC interface. When logged into a KX unit as an Administrator, you can perform the following administrative tasks directly from RRC.

---

### Firmware Upgrade

On the **Tools** menu, click **Update Device** to perform firmware upgrades.

RRC will prompt you to locate a Raritan firmware distribution file (\*.RFP format), found on the Raritan web site (www.raritan.com) when available. Be sure to read all instructions included in firmware distributions before performing an upgrade.

---

### Device Restart

Select a device in the RRC Navigator, and on the **Tools** menu, click **Restart Device** to restart the KX unit.

---

### Device Configuration Backup and Restore

On the **Tools** menu, click **Save Device Configuration** to download the KX device configuration to your local computer.

On the **Tools** menu, click **Restore Device Configuration** to upload the archived KX device configuration.

Please note that the device configuration is specific to a particular device and should not be restored to another KX device.

---

### User Configuration Backup and Restore

On the **Tools** menu, click **Save User Configuration** to download the Dominion KX device configuration to your local computer.

On the **Tools** menu, click **Restore User Configuration** to upload the archived Dominion KX configuration.

Use these functions to transfer user and group information from one KX unit to another.

---

### Log Files

On the **Tools** menu, click **Save Activity Log** to download a detailed activity log for troubleshooting purposes.

On the **Tools** menu, click **Save Diagnostic Log** to download a detailed diagnostic log for viewing, reporting, and analysis.

## Broadcast Port

By default, all Raritan devices send data through Port 5000. This network traffic includes RRC's auto-discovery broadcast. In the case of conflicts, or to deal with firewall issues, you may wish to use a different broadcast port.

To change the default broadcast port, on the **Tools** menu, click **Options**. Type the new port number at the bottom of the window, and then click **OK** to accept the changes.

*Note: If you wish RRC to continue auto-discovering Raritan devices on the new broadcast port, you must configure those devices to use the new port number.*

## Remote Power Management

With a properly configured Raritan Remote Power Control Strip, RRC can manage AC Power to associated targets by providing three options for the remote power management of targets: **Power On**, **Power Off**, and **Cycle Power**.

To change the power status of a target:

1. Select the target server in RRC's Navigator Window in the left panel of your screen.
2. Right-click on the target server, and if the target server is associated with an outlet on a Remote Power Control Strip, choose **Power On**, **Power Off**, or **Cycle Power** to the target, as needed (these commands are also part of the RRC **Tools** drop-down menu).

## General Options

1. On the **Tools** menu, click **Options** to view the Options screen. You can customize your keyboard and video options to optimize use of RRC.

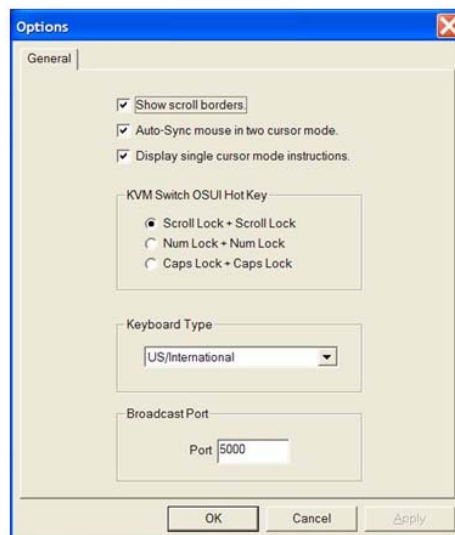
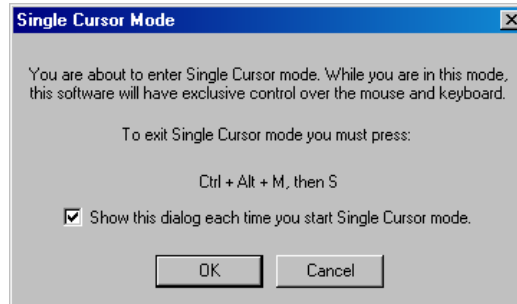


Figure 44 RRC Options Panel

2. Click on the check box before **Show scroll borders** to view the thin scroll borders that show the Auto-Scroll area.
3. Click on the check box before **Auto-Sync mouse in two cursor mode** to enable Automatic Mouse Synchronization.

4. Click on the check box before **Display Single cursor mode instructions** if you wish to see the following instructions when entering Single Cursor Mode.



*Figure 45 Single Cursor Mode Confirmation Screen*

5. In the KVM Switch OSUI Hot Key panel, click on the radio button before your choice of hot key combinations.
6. In the Keyboard Type panel, click on the drop-down arrow and click on your keyboard choice.
7. In the Broadcast Port Panel, type the broadcast port number in the Port field.
8. Click **OK** when finished or click Cancel to exit this window without saving changes. Click Apply any time during your selection to apply an option you have chosen.





## Chapter 4: Administrative Functions

Dominion KX Manager is used to manage both the Dominion KX and the KX101 product lines. When running on either a Dominion KX or a KX101, features specific to the other unit are disabled.

### Launching Dominion KX Manager

Launch KX Manager in one of three ways:

- Launch via RRC/MPC by clicking on the “admin” port on a device.
- Launch directly from a Web browser (if you have the IP address of the device).
- Launch KX Manager as an application on Windows and Linux OS. Start the installer to install KXM; KXM is then accessible from the Start menu (click Start, then click Programs, and then select Dominion Manager).

If you are using Internet Explorer (IE), launch your browser and type the URL:

**http://IP-ADDRESS/admin**

If you are using Netscape version 7.1 or higher, launch your browser and type the URL:

**http://IP-ADDRESS/admin.html**

where **IP-ADDRESS** is the IP Address assigned to your KX device. A browser will prompt you to grant permission to retrieve and launch KX Manager. After you grant permission, KX Manager launches.



Figure 46 Dominion KX Manager Login Screen

**Username / Password:** Log on to KX Manager with the username and password of any user with Administrative privileges.

---

**Note:** The default login user name is **admin** with the password **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 in lowercase letters. To ensure security, change the default username password as soon as possible.

---

**Port:** If your device has been configured to use a different TCP port than the default port 5000, type that number here.

## KX Manager Interface

KX Manager provides an interface for performing configuration and administrative functions. Many commands in the drop-down menus can be accessed by right-clicking on icons in the server and user lists on the left side of the screen.

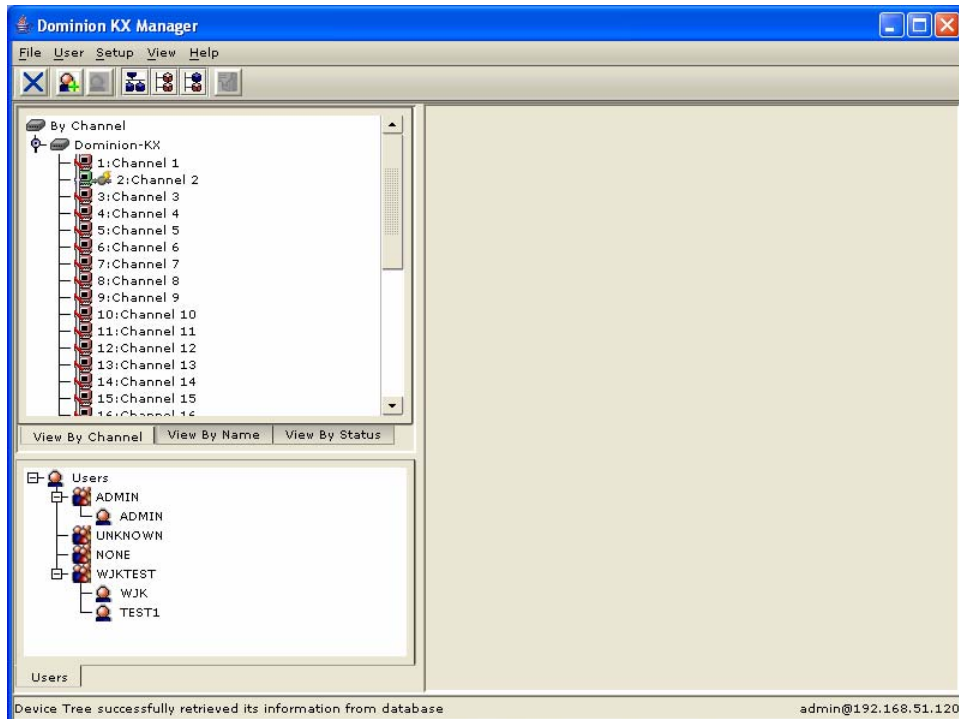


Figure 47 KX Manager Main Screen

There are three ways to view channels; click on the tabs to change your view:

- View by Channel (number)
- View by Name
- View by Status – when viewing channels by Status, channels appear in the following order, sorted alphanumerically:
  - Busy Channels
  - Available Channels
  - Unavailable Channels

## Network Configuration

Use these descriptions to customize the network configuration settings, such as IP Address, Ethernet speed, and others, on your Dominion KX unit.

---

Important: The device must be rebooted before Network Configuration changes take effect.

---

1. On the **Setup** menu, click **Configuration**, and then click **Network**. The **Network Configuration** window appears.

The screenshot shows the 'Network Configuration' window with the following fields and options:

- Manager name:** Text box containing 'Dominion-KX'.
- Line speed & duplex:** Dropdown menu set to 'Auto detect'.
- Obtain IP address automatically (DHCP):** Unchecked checkbox.
- Addresses and masks:**
  - IP address:** Text box containing '192.168.51.120'.
  - Subnet mask:** Text box containing '255.255.255.0'.
  - Default gateway:** Text box containing '192.168.51.126'.
  - Use default TCP port 5000:** Checked checkbox.
  - Port:** Text box containing '5000'.
- Buttons:** 'Set System ACL...' button.
- Failover:**
  - Enable automatic failover:** Unchecked checkbox.
  - Ping interval (secs):** Text box containing '30'.
  - Timeout (secs):** Text box containing '60'.
- Interfaces:**
  - Enable modem interface:** Unchecked checkbox.
- Enable syslog forwarding:** Unchecked checkbox.
- Syslog:**
  - Remote IP address:** Empty text box.
  - Category:** Dropdown menu set to 'Network'.
  - Priority threshold:** Dropdown menu set to 'Emergency'.
- SNMP:**
  - Enable SNMP:** Unchecked checkbox.
- Bottom buttons:** 'OK', 'Cancel', and 'Help' buttons.

Figure 48 Network Configuration Window

Some parameters that may be unfamiliar:

- **Manager Name:** Type a unique name for the device. The default name for a Dominion KX unit is: “**Dominion-KX**” and for a KX101 unit is **KX\_KIM-*<last five digits of serial number>***, for example, a KX101 with serial number S00002 would have a default name of **KX\_KIM-00002**. Remote users will see and use this name to identify this particular device. However, if an RRC user has created a Connection Profile for a device, that user will see the **Description** field from the Profile instead.

---

**Note:** Spaces are **NOT** permitted in the Manager Name.

---

- **Enable Modem Interface:** (Dominion KX only) Enables the device’s internal modem port to allow remote users to dial into the device. Default value = Disabled.
- **Use Default TCP Port 5000:** Besides the initial download of Raritan Remote Client and KX Manager (which occurs over secure HTTPS Port 443), all communication to and

from the Dominion KX occurs over a single, configurable TCP Port. The default is Port 5000, but you can configure it to use any TCP port except 80 and 443. To access the KX unit from beyond a firewall, your firewall settings must enable two-way communication through the default port 5000 or the non-default port configured above.

- **Enable Syslog Forwarding:** Click on this check box to the device's log messages to a remote syslog server. Type the IP Address of your syslog server in the **Remote IP Address** field and click on the **Category** and **Priority Threshold** drop-down arrows to select the level of event sensitivity.
- **Set System ACL:** Click to set a global-level access control list for your KX unit by ensuring that your device does not respond to packets being sent from disallowed IP addresses. The Access Control List window appears.

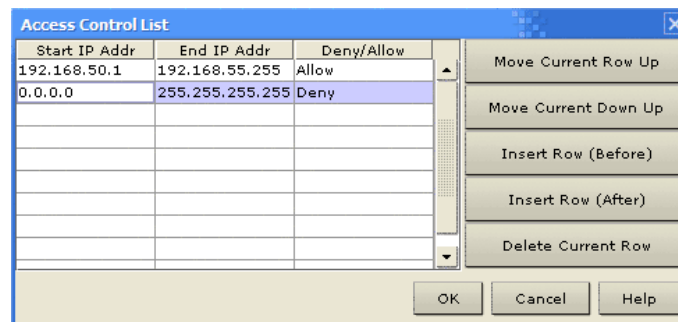


Figure 49 Access Control List Window

- These ACL values are global, affecting the KX unit as a whole. Your device allows you to create ACLs for each user group, for example, you can create a user group “Outsourced Vendors,” that is permitted to access Dominion KX only from a given IP address range (please see the section **Users, Groups, and Access Permissions** in this chapter, for more information on how to create group-specific ACLs).
- Click **OK** to accept the Access Control List changes or **Cancel** to close the window without saving changes.

---

Important: Please note that ACL rules are evaluated in the order in which they are listed. For instance, if in the above example, the two ACL rules were reversed, Dominion KX101 would accept no communication at all. Use the buttons on the right of the window to adjust the order of your list.

---

- **Enable Automatic Failover:** (Dominion KX only) Click on this check box to allow Dominion KX to automatically recover its network connection using a second network port if the active network port fails. **Ping Interval** determines how often Dominion KX will check the status of the network connection (setting this too low may cause excess network traffic). **Timeout** determines how long a network port must be “dead” before the switch is made. Both network ports must be connected to the network and this option must be checked for Automatic Failover to function.
  - **SNMP:** (KX101 only) Enable or Disable KX101 to send out SNMP status.
2. Click **OK** to set Network Configurations or click **Cancel** to close the window without saving changes.

3. When the **Confirm action** window appears, click **Restart Now** to save changes to the KX unit and restart the device, click **Restart Later** to save changes and restart the device at a later time (please note that some changes require restarting the device), or click **Cancel** to return to the previous window..

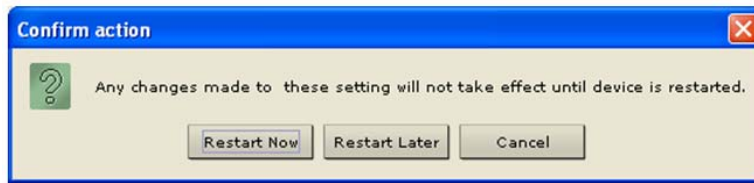


Figure 50 Confirm Action Window

### Reset Settings to Default

To delete all of the configured device's network settings and return to factory default settings, use the **Local Console Port** to reset all network settings.

- To delete all configured Dominion KX network settings, use the local OSD or the reset option on the Diagnostics screen.

## System-Level Security Parameters

Use these descriptions to change system-level security settings, such as encryption levels, idle time, share mode, and other parameters.

---

**Important:** The device must be rebooted before Network Configuration changes take effect.

---

1. On the **Setup** menu, click **Security**, and then click **Setting**. The **Security Settings** window appears.



Figure 51 Security Configuration Window

- **Encryption mode** – click on the drop-down arrow to select one of the following:
  - **SSL authentication, NO data encryption:** Usernames and passwords are secured, but KVM transmissions are not. 128-bit Secure Socket Layer (SSL) protocol provides a private communications channel between the KX unit and the Remote PC during initial connection authentication. No encryption security in place during remote KVM data transfer.
  - **SSL authentication, data encryption:** Secures user names, passwords and KVM data, including video transmissions. 128-bit Secure Sockets Layer (SSL) protocol provides a private communications channel between the KX unit and the Remote PC during initial connection authentication. After authentication, KVM data is also transferred with 128-bit encryption, but using a protocol much more efficient than SSL (RC4 encryption, but without SSL headers). Raritan recommends this option.
  - **SSL authentication, SSL data encryption:** Secures user names and passwords, and provides high-level security for KVM data. 128-bit Secure Sockets Layer (SSL) protocol provides a private communications channel between the KX unit and the Remote PC during initial connection authentication. 128-bit SSL encryption is also in place during remote KVM data transfer. Note that because the SSL protocol was

not designed for KVM communication, this mode is less efficient but no more secure than the recommended setting, above.

- **PC Share Mode** – Determines global concurrent remote access, enabling up to eight remote users to simultaneously log on to one KX unit and concurrently view and control the same target server through the device. Click on the drop-down arrow to select one of the following:
  - **Private Mode (default):** No PC Share. Each target server can be accessed exclusively by only one user at a time.
  - **PC Share Mode:** Target servers can be accessed by eight users (administrator or non-administrator) at one time. Control is based on first active keyboard/mouse input, so multiple remote users attempting keyboard input or mouse movement at exactly the same moment may experience uneven control.
 

**Note:** PC Share Mode is a global setting. For individual user access settings see **Keyboard and Mouse Control** and **Concurrent Access Mode** on the **User Account Settings** screen. Each user profile can be set individually to enable/disable keyboard and mouse control, and concurrent access.
- **Log Out Idle Users:** Click on the check box to automatically disconnect remote users after a certain amount of inactive time has passed. Type the amount of time in the **After** field.

---

***Note:** If you invoke KX Manager via the **Admin** channel in RRC, be aware that this timer can affect your session. Launch KX Manager outside of RRC or disable this parameter for the session to avoid having RRC's user idle time logout your KX Manager session.*

---

- **Enable Strong Passwords:** Requires user passwords to have a minimum of 6 characters with at least one alphabetical character and one non-alphabetical character (punctuation or number). The first four characters of the password and the username cannot match. Strong password rules affect only those usernames and passwords stored by Dominion KX. If you configure the device to authenticate to a remote server such as LDAP, RADIUS, or Active Directory, these rules are not enforced by the device (please see the section **Remote Authentication** in this chapter for more information on remote authentication).
- **Enable Multiple Logins:** When this rule is selected, a given username/password combination can be connected into the device from multiple client workstations at a time.
- **Password Expiration Time:** Type a number of days in this field to force users to change their passwords after a set duration.
- **Private Key:** Type a private key password. Only those remote users who know the private key, in addition to their own usernames and passwords, can log in and connect to the device.
- **Re-Enter Private key:** Type private key password again for confirmation. Remember that passwords are case sensitive. Private key passwords must be alphanumeric; special characters cannot be used.
- **Local Device Reset Mode:** Determines how the Admin password recovery process operates. Click on the drop down arrow to select one of the following:
  - **Enable local factory reset** (Default)
  - **Enable local admin password reset**
  - **Disable all local resets**

For the password recovery process, refer to “**Administrator Password**” in **Chapter 2: Installation** of this document.

2. Click **OK** to set Security Configurations or click **Cancel** to close the window without saving changes.

## Time and Date

The Time and Date screen allows you to access the device's current settings to set time, date, time zone, adjustment for Daylight Savings, and Network Time Protocol (NTP).

**Time and Date**

**Time and Date**

Date: June 2005

Sun	Mon	Thu	Wed	Thr	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Adjust for daylight savings time

Current time: **14:28:18**

Hours: 14

Minutes: 28

Seconds: 14

Get time from NTP server

NTP server

Primary server IP address: 0.0.0.0

Secondary server IP address:

Use standard UDP port 123

NTP time server port: 123

Time Zone: (GMT-05:00) Eastern Time Zone (US & Canada)

OK Cancel Help

Figure 52 Time and Date Settings



## Users, Groups, and Access Permissions

### Overview

---

The device stores an internal list of user and group names to determine access authorization and permissions. This information is stored internally in a hashed / encrypted format.

#### Note to CommandCenter Users

If you plan to configure the device to be integrated with and controlled by Raritan's CommandCenter management appliance, this section of the User Manual does not apply to you. When the device is controlled by CommandCenter, CommandCenter determines the allowed users and groups. Please refer to your CommandCenter User Guide.

#### Note to Raritan Customers Upgrading from Previous Firmware Versions

If you previously configured Raritan products such as Dominion KSX and IP-Reach running legacy firmware versions earlier than v3.2, read this entire section carefully. Beginning with firmware version v3.2 and above, the implementation of users and groups has changed significantly to provide more flexible and powerful configurations.

### Relationship between Users and Group Entries

---

You may want to organize users in your device into groups. Assigning users to 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.

**User information** helps in authenticating users accessing your KX unit. 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.

You may choose not to associate specific users with groups. In this case, the KX unit classifies the user as “**Individual.**”

The user list on the left side of the screen displays both User and Group names created for the device. Users belonging to a Group are nested under their group name.

#### Mandatory User Groups

Every Dominion KX unit has three default user groups, which cannot be deleted:

ADMIN	User group for original, factory-default administrative user.
NONE	Permissions defined for this group are employed for a user when your Dominion KX is configured for remote authentication via LDAP or RADIUS (see next section), and a login attempt is successful but no user group is returned by the remote authentication server.
UNKNOWN	Permissions defined for this group are employed for a user when your Dominion KX is configured for remote authentication via LDAP or RADIUS (see next section), and a login attempt is successful but the user group returned by the remote authentication server is not found in Dominion KX.

## Create or Edit User Groups and Access Permissions

Define User Groups before creating individual Users. When creating a user, you must assign that user to an existing user group. In addition, User Groups are used even if you implement remote authentication (via RADIUS or LDAP).

1. **To create a new User Group:** On the **User** menu, click **Add User Group**. **To edit an existing User Group:** Select the group that you wish to edit in the user list, right-click on the icon, and select **Edit User Group**. Either the **Add Group** or the **Edit Group** window appears.

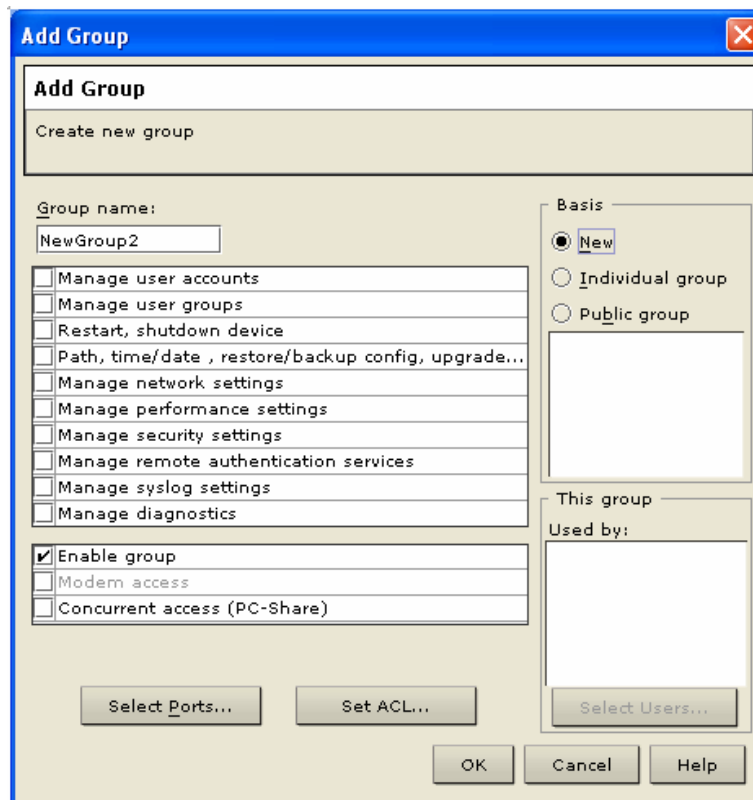


Figure 53 Add Group Window

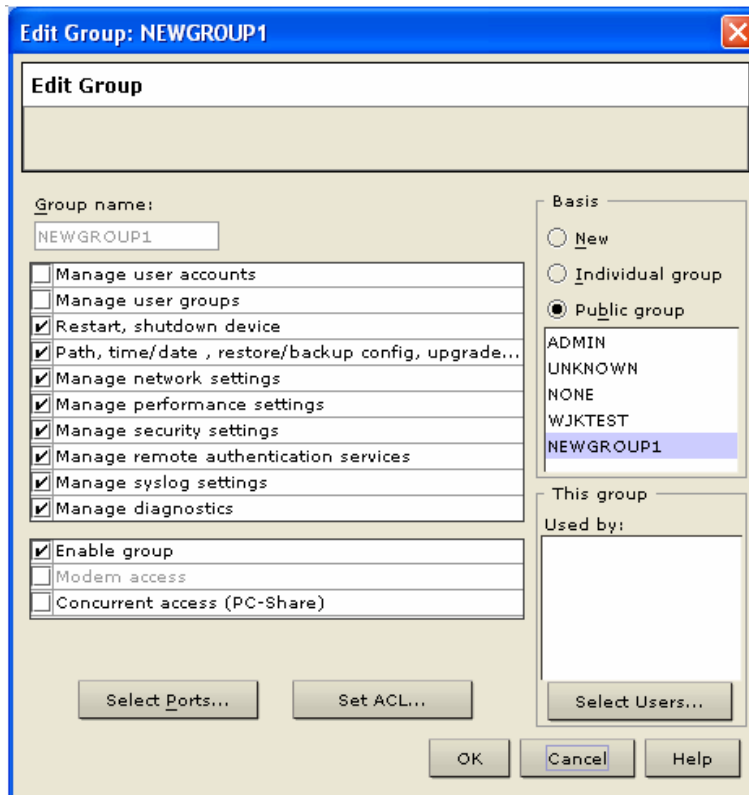


Figure 54 Edit Group Window

2. Type a name for the new user group, or edit the name for an existing user group in the **Group Name** field.
3. Check the boxes before the permissions you want to assign to all users who belong to this group.
4. In the **Basis** panel of the screen, click on the radio button before one of the options to indicate this is a **New** group, to specify it as an **Individual** group, or to copy the permissions from an existing **Public** group. If you select **Public** group, the names of currently existing groups appear in the field below; click on one of them to apply that group's properties to the group you are adding.
5. The first group of permissions (the upper table) controls user authorization for using these specific administrative functions within KX Manager; for example, if you check the box before **Manage user accounts**, the members in this group can create new user accounts in KX Manager. Several administration functions are available within RRC and from Dominion KX's Local Console Port; these functions are available only to members of the default ADMIN group. Please note that if you enable **Manage user accounts** and **Manage user groups**, confirmation windows appear so that you can confirm your choice. Click **OK** to continue.
6. In the second group of permissions (the lower table), uncheck **Enable Group** to disable all access and permissions for members of this group. Check **Concurrent Access (PC Share)** to allow group members simultaneous log-on capability to Dominion KX with concurrent view and control of targets, such as a PC Share session. (**Modem Access** is disabled in KX101.)

---

Important: Enabling Manage user accounts and Manage user groups permissions allows the members of the group to change the permissions of all users, including their own. Carefully consider granting these permissions.

---

7. Other permission elements on the Add Group or Edit Group screens include:
- **This Group** panel, **Used By** field - Displays all users assigned to this group. The **Select Users** button allows administrators to move previously configured users into this group.
  - **Select Ports** – Click this button to specify which server ports can be accessed by users who belong to this group. For each server port, users may be allowed to control the connected target server; view the video (but not interact with) the connected target server; or be denied permission altogether.

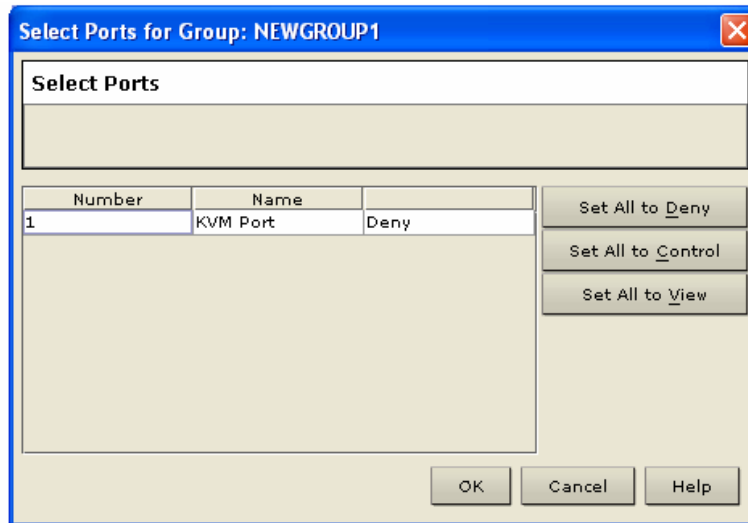


Figure 55 Select Ports Window

- **Set ACL** – Click this button to limit access to the device by users in this group to specific IP addresses. (This feature applies **only** to users belonging to a specific group, unlike the “Set System ACL” functionality found in the device’s Network Configuration (see previous section **Network Configuration**), which applies to **all** access attempts to the device).

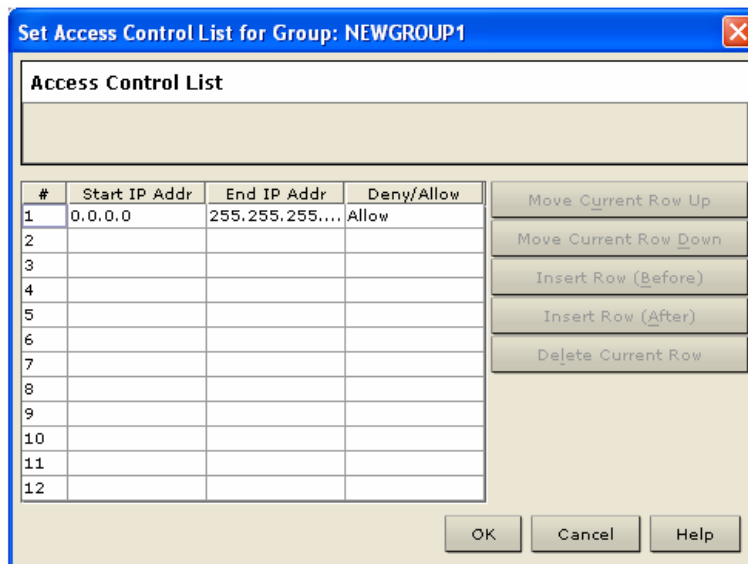


Figure 56 Set Access Control List for Group Window

---

Important: Please note that ACL rules are evaluated in the order that they are listed.

---

8. Click **OK** to save Group properties or click **Cancel** to close the window without saving.

## Moving Users between Groups

---

To organize users into groups, select the user group you want to modify, and on the **User** menu, click **Add User to Group** (or click [**Select Users**] in the Groups window).

When the **Select Users** screen appears, add users to the group by selecting the user in the **All Users** list and clicking **→** to move the user to the **Users in Group** list. To remove users from the group, select the user in the **Users in Group** list and click **←** to move the user to the **All Users** list.

## Delete User Groups

---

To delete existing user groups, select the group that you wish to delete, right-click on the group icon, and select **Delete User Group**. Before deleting a group, ensure that there are no users assigned to it, or those users will also be deleted.

## Create or Edit Users

---

1. **To create a new User:** On the **User** menu, click **Add User**. **To edit an existing User:** Select the user that you wish to edit in the user list, right-click on the icon, and select **User Properties**. The **Add User** or the **Edit User** window appears:

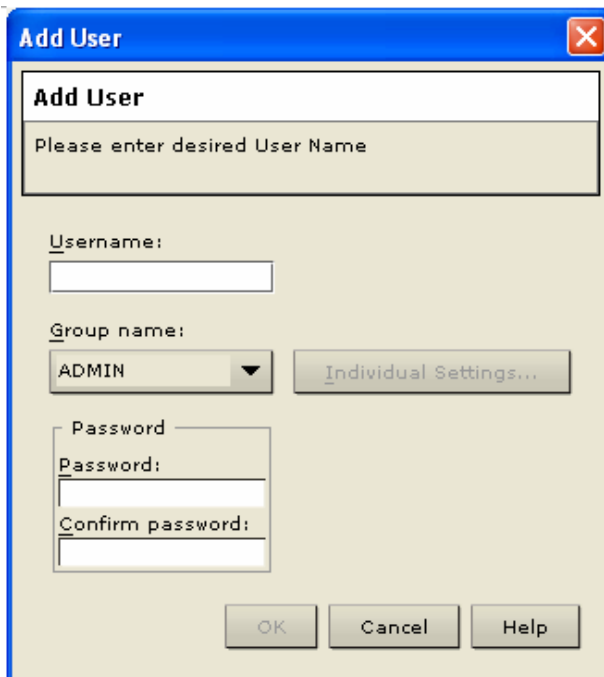
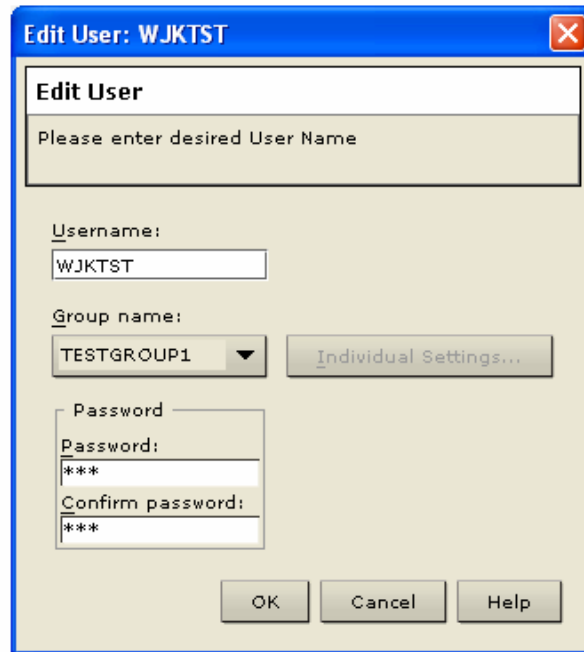


Figure 57 Add User Window



The image shows a Windows-style dialog box titled "Edit User: WJKTST". The dialog has a blue title bar with a close button (X) in the top right corner. The main area is light gray and contains the following elements:

- A header section with the title "Edit User" and a message: "Please enter desired User Name".
- A "Username:" label followed by a text input field containing "WJKTST".
- A "Group name:" label followed by a dropdown menu showing "TESTGROUP1" and a button labeled "Individual Settings...".
- A "Password:" label followed by a text input field containing "\*\*\*".
- A "Confirm password:" label followed by a text input field containing "\*\*\*".
- At the bottom, there are three buttons: "OK", "Cancel", and "Help".

Figure 58 Edit User Window

2. Type a unique user name or edit the existing user name in the **Username** field.
3. Click on the **Group Name** drop-down arrow and select a User Group to which you want to assign this user. If you do not want to associate this user with an existing User Group, select **Individual Group** from the drop-down list, and then click **Individual Settings** to assign access permissions and privileges for this user.
4. Type a new password or edit an existing password in the **Password** field. Retype the password in the **Confirm Password** field. Any character can be used to create a password.
5. Click **OK** to save User properties or click **Cancel** to close the window without saving.

## Delete Users

---

To delete an existing user, select the user that you wish to delete, right-click on the user icon, and select **Delete User**.

# Remote Authentication

## Introduction

---

### Note to CommandCenter Users

If you plan to configure the device to be integrated with and controlled by Raritan's CommandCenter management appliance, this section of the User Manual does not apply to you. When a device is controlled by CommandCenter, CommandCenter determines the allowed users and groups. Please refer to your CommandCenter User Guide.

### Note to Raritan Customers Upgrading from Previous Firmware Versions

If you have previously implemented RADIUS authentication on Raritan products such as Dominion KSX and IP-Reach running legacy firmware versions earlier than v3.2, read this entire section carefully. Beginning with firmware version v3.2 and above, the implementation of external authentication has changed significantly to provide more flexible and powerful configurations.

### Supported Protocols

In order to simplify management of usernames and passwords, device provides the capability to forward authentication requests to an external authentication server. The device supports two external authentication protocols: LDAP and RADIUS.

### Note on Microsoft Active Directory

Microsoft Active Directory uses the LDAP protocol natively, and can function as an LDAP server and authentication source for KX101. If it has the IAS (Internet Authorization Server) component, a Microsoft Active Directory server can also serve as a RADIUS authentication source.

## Remote Authentication Implementation

---

### Priority

When a user tries to authenticate to a KX101 unit that is configured for external authentication, KX101 first checks its own internal user database for that username. If the username is not found in the KX101 internal database, the request is forwarded to the external authentication server.

- **If Username is not found in the KX101 internal database:** Request is forwarded to external authentication server to determine whether the login is allowed or denied.
- **If Username is found in the KX101 internal database and Password is correct:** Login is allowed.
- **If Username is found in the KX101 internal database and Password is incorrect:** Login is denied; the request does NOT get forwarded to the external authentication server.

## Authentication vs. Authorization

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

Authorization is determined by the KX unit on the basis of user groups. That is, once a given user is allowed to access the device in general (authenticated), that user's specific permission (authorization) is determined by the device, based upon the user's group.

The external authentication server can assist in authorization by informing the device about the user group to which a user belongs whenever the authentication server approves a given user's login request. The sections **Implementing LDAP Remote Authentication** and **Implementing RADIUS Remote Authentication** that follow explain this in more detail.

This is most easily described via a simple flow diagram:

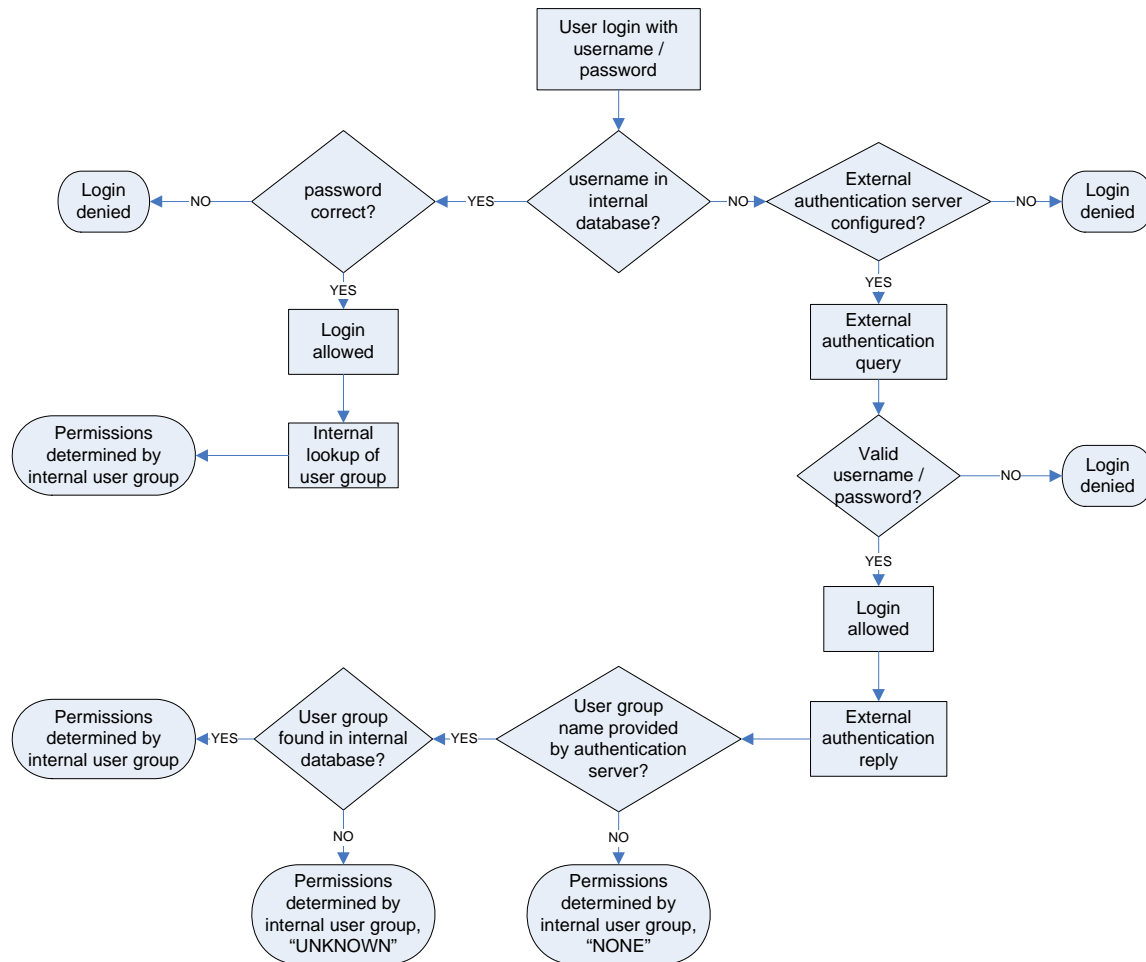


Figure 59 Authorization Flow Diagram

Note the importance of the group to which a given user belongs, as well as the need to configure the groups named, “UNKNOWN” and “NONE.” If the external authentication server returns a group name that is not recognized by the KX101, that user's permissions are determined by the permanent group named “UNKNOWN.” If the external authentication server does not return a group name, that user's permissions are determined by the permanent group named “NONE.”

Please see the section **General Settings for Remote Authentication** in this chapter to determine how to configure your authentication server to return user group information to KX101 as part of its reply to an authentication query.



## General Settings for Remote Authentication

1. On the **Setup** menu, click **Security**, and then click **Remote Authentication** to configure KX101 unit for remote authentication. The **Remote Authentication** window appears:

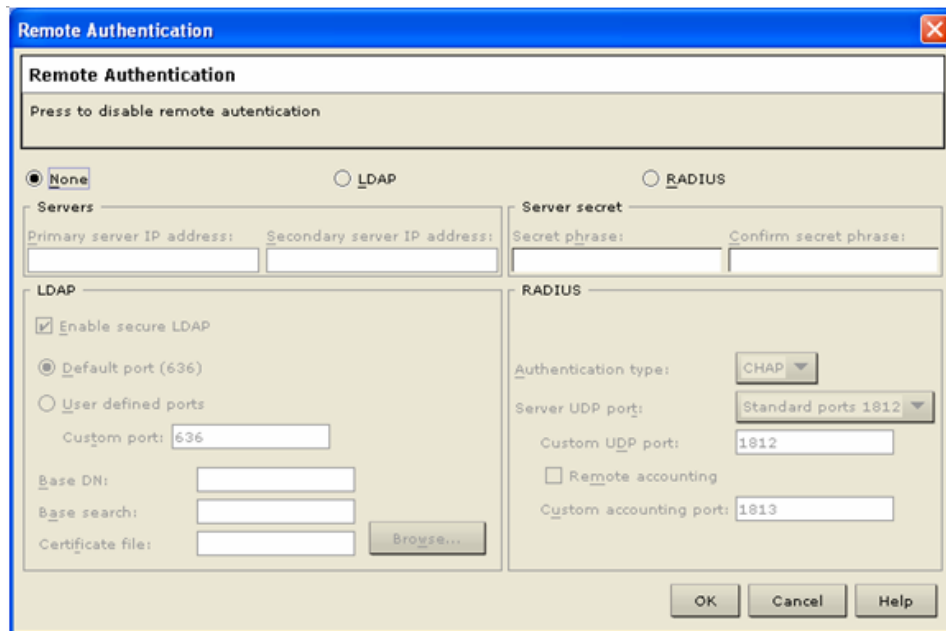


Figure 60 Remote Authentication Window

2. Select the option button of the remote authentication protocol you prefer (**LDAP** or **RADIUS**).
3. Type the IP Address of your primary and secondary remote authentication servers in the **Primary Server IP Address** and **Secondary Server IP Address** fields.
4. Type the server secret needed to authenticate against your remote authentication servers in the **Secret Phrase** field. Re-type the server secret in the **Confirm Secret Phrase** field.
5. If you selected LDAP as your remote authentication protocol, please read the next section **Implementing LDAP Remote Authentication** to complete the fields in the LDAP panel of the Remote Authentication window. If you selected RADIUS, please skip to **Implementing RADIUS Remote Authentication** to complete the fields in the RADIUS panel of the window.
6. When finished, click **OK** to save the Remote Authentication changes or click **Cancel** to exit without saving.

### Implementing LDAP Remote Authentication

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

If you choose LDAP authentication protocol, complete the LDAP fields as follows:

- **Use Secure LDAP:** Apply this rule to enables LDAP-S, which ensures that all authentication requests and replies transmitted over the network are encrypted.
- **Default Port / User Defined Port:** Select an option button to choose whether you would like to use the standard LDAP TCP ports, or specify your own user defined port.
- **Base DN, Base Search:** 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 DN value might be: “cn=Administrator,cn=Users,dc=testradius,dc=com” and 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.

- **Certificate File:** Consult your authentication server administrator for the appropriate values to type into this field in order to process LDAP authentication queries from Dominion KX101.

### Returning User Group Information via LDAP

When an LDAP authentication attempt succeeds, Dominion KX101 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 server. Please consult your authentication server administrator to enable this attribute.

### Returning User Group Information from Microsoft Active Directory

Returning user group information from Microsoft's Active Directory for Windows 2000 Server requires updating the LDAP schema. This should be attempted only by an experienced Active Directory administrator. Please refer to your Microsoft documentation for more detail.

#### To Begin

- Install the schema plug-in for Active Directory – please refer to Microsoft Active Directory documentation for instructions.
- 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.

#### Setting the Registry Key

1. Right-click the **Active Directory Schema** root node in the left pane of the window, and then click **Operations Master**.
2. Click on the check box before **The Schema may be modified on this Domain Controller**.
3. Click **OK**.

## Creating a New Attribute

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

1. Click the + symbol before **Active Directory Schema** in the left pane of the window.
2. Right-click **Attributes** in the left pane.
3. Click **New**, and then select **Attribute**. When the warning message appears, click **Continue** and the **Create New Attribute** window appears.

Figure 61 Creating a New Attribute

4. Type **rciusergroup** in the **Common Name** field.
5. Type **rciusergroup** in the **LDAP Display Name** field.
6. Type **1.3.6.1.4.1.13742.50** in the **Unique x500 Object ID** field.
7. Click on the **Syntax** drop-down arrow and select **Case Insensitive String** from the list.
8. Type **1** in the **Minimum** field.
9. Type **24** in the **Maximum** field.
10. Click **OK** to create the new attribute.

## Adding Attributes to the Class

1. Click **Classes** in the left pane of the window.
2. Scroll to the **user** class in the right pane, and right-click on it.
3. Select **Properties** from the menu. The **user Properties** window appears.
4. Click on the **Attributes** tab.
5. Click **Add**.
6. Select **rciusergroup** from the **Select Schema Object** list.

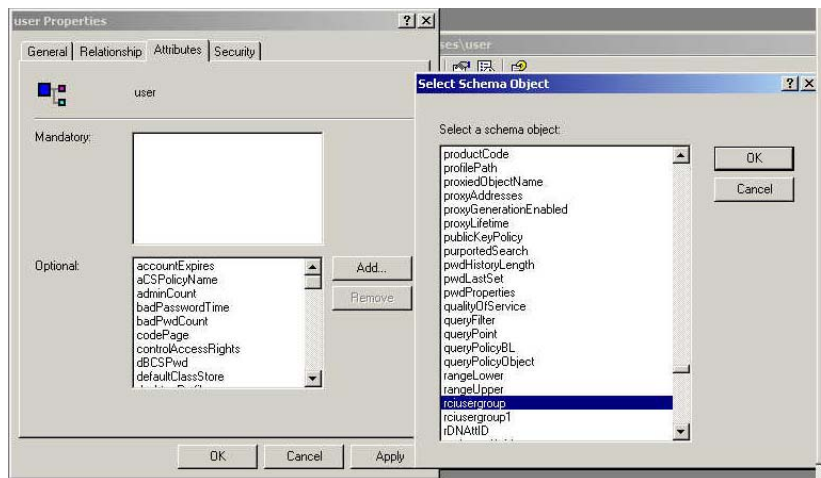


Figure 62 Adding the Attributes to the Class

7. Click **OK**.
8. Click **OK**.

### Updating the Schema Cache

9. Right-click **Active Directory Schema** in the left pane of the window and select **Reload the Schema** from the shortcut menu.
10. Minimize the Active Directory Schema MMC console.

### Adding Values to New Attributes

---

The following is applicable for Microsoft 2000 servers only.

---

Run the Raritan script **Addmenu.vbs**.

This script can be downloaded from Raritan's web site. Please launch your browser and type the following URL [http://www.raritan.com/support/sup\\_technotes.aspx](http://www.raritan.com/support/sup_technotes.aspx). Scroll to the Dominion KX section, click on the **Active Directory Addmenu.zip** file, and follow the instructions to download the file to your machine.

### Modifying New Attributes

---

The following is applicable for Microsoft 2000 servers only.

---

Use the **Active Directory Users and Computers** snap-in to modify the new attributes for users.

1. On the **Start** menu, click **Programs**, select **Administrative Tools**, and then click **Active Directory Users and Computers**. Click on the *Specific User Name* to select it.
2. Right-click on the *Specific User Name*, and click **Raritan KX User Group**. A small VBScript application starts that allows you to modify the user's rciusergroup value.
3. Type **admin** or the KX user group name you would like returned to RRC.
4. Click [**OK**].

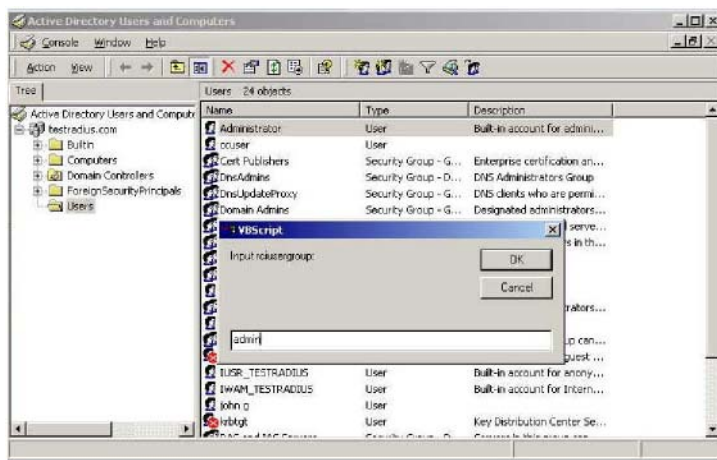


Figure 63 Entering the User Group Name to be Returned

## Editing RCI User Group Attributes for User Members

The following is applicable for Microsoft 2003 servers only.

To run Active Directory script on Windows 2003 server, please use the script provided by Microsoft. These scripts are loaded onto your system with a Microsoft Windows 2003 installation. ADSI, or 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. For additional information, visit Microsoft's Web site: <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/ebca3324-5427-471a-bc19-9aa1decd3d40.msp>.

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

1. On the Windows **Start** menu, click **Run**.
2. Type **regsvr adsiedit.msc**. The ADSI Edit window appears.

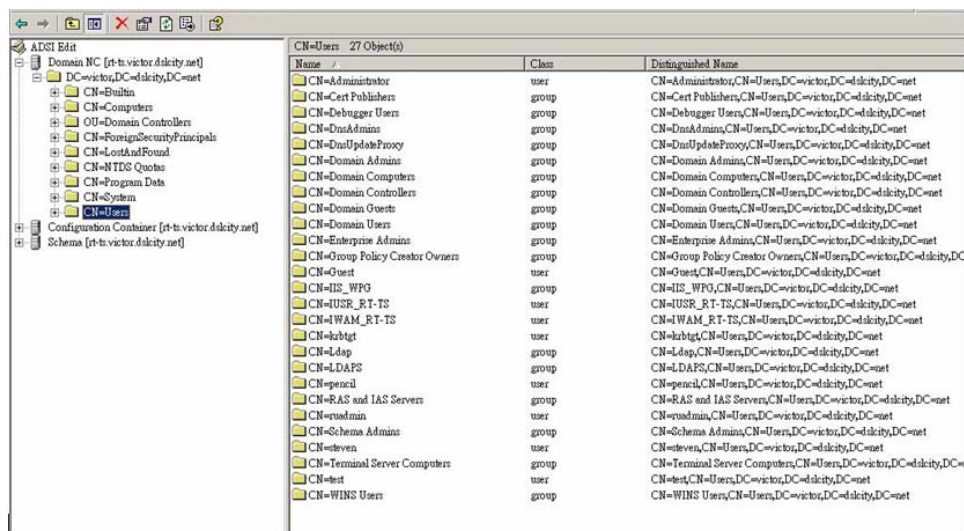


Figure 64 ADSI Edit Window

3. In the left pane of the window, select the **CN=User** folder.
4. Locate the user name whose properties you want to adjust in the right pane. Right-click on the user name and select **Properties**.

5. Click on the **Attributes** tab.
6. Click on the **Select a property to view** drop-down arrow and select **rciusergroup** from the list.

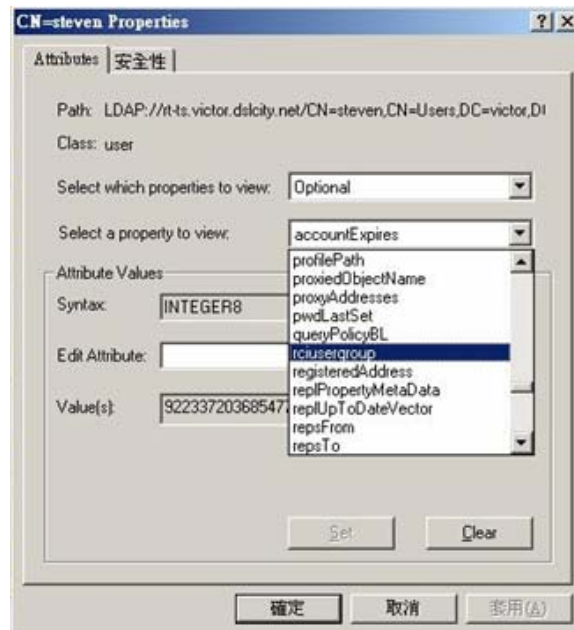


Figure 65 User Properties Screen

7. In the **Attribute Values** panel of the window, type the user name you would like returned to RRC in the **Edit Attribute** field.

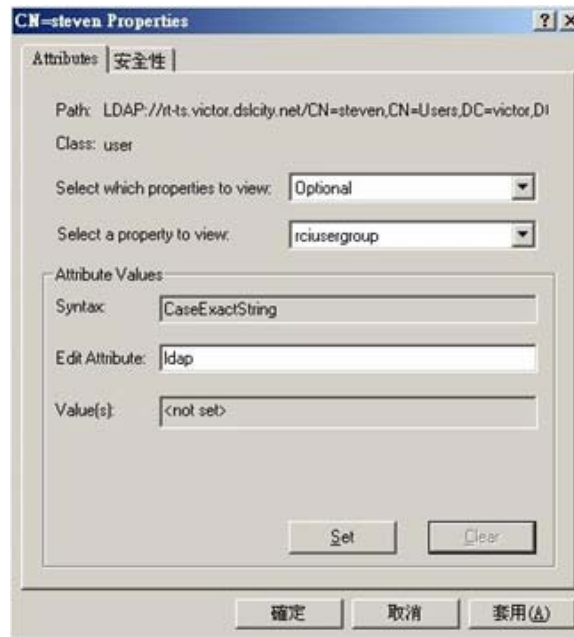


Figure 66 Edit Attribute - adding user to KX group

8. Click **Set**.
9. Click **OK**.

## Implementing RADIUS Remote Authentication

Microsoft Active Directory can be used as source information for RADIUS authentication by installing the Windows server component **Internet Authentication Server**.

If you choose RADIUS authentication protocol, complete the RADIUS fields as follows:

- **Authentication Type:** Click on the drop-down arrow to select either CHAP or PAP protocol.
- **Server UDP Port / Custom UDP Port:** Click on the drop-down arrow to select whether you would prefer using standard RADIUS TCP port 1812, the legacy RADIUS TCP port 1645, or type in your own user defined port in the **Custom UDP Port** field.
- **Remote Accounting / Custom Accounting Port:** Click on the check box to send authentication events to a RADIUS accounting server; if so, type the TCP port should be used for transmitting events in the **Custom Accounting Port**.

### Returning User Group Information via RADIUS

When a RADIUS authentication attempt succeeds, the 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

KX101 sends the following information to RADIUS server in an authentication query:

ATTRIBUTE	DATA
USER-NAME	The user name entered at the login screen.
USER-PASSWORD	In PAP mode, the encrypted password entered at the login screen.
CHAP-PASSWORD	In CHAP mode, the CHAP protocol response computed from the password and the CHAP challenge data.
NAS-IP-ADDRESS	Dominion KX's IP Address
NAS-IDENTIFIER	The Dominion KX unit name as configured in "Network Configuration" (see previous section).
NAS-PORT-TYPE	The value ASYNC (0) for modem connections and ETHERNET (15) for network connections.
NAS-PORT	Always 0.
STATE	If this request is in response to an ACCESS-CHALLENGE, the state data from the ACCESS-CHALLENGE packet will be returned.
PROXY-STATE	If this request is in response to an ACCESS-CHALLENGE, the proxy state data from the ACCESS-CHALLENGE packet will be returned.

KX101 unit sends the following RADIUS attributes to the RADIUS server with each accounting request:

ATTRIBUTE	DATA
SESSION-TYPE	Either START (1) for log in or STOP (2) for log out.
SESSION-ID	A string containing a unique session name. The name is in the format of “NAS-IDENTIFIER:user IP address:unique session number” Example: “Dominion KX:192.168.1.100:122”
USER-NAME	As above.
NAS-IP-ADDRESS	As above.
NAS-IDENTIFIER	As above.
NAS-PORT-TYPE	As above.
NAS-PORT	As above.
FILTER-ID	Any FILTER-ID attributes returned by the RADIUS server during authentication will be sent in each accounting request.
CLASS	Any CLASS attributes returned by the RADIUS server during authentication will be sent in each accounting request.
ACCT-AUTHENTIC	How the user was authenticated. Either RADIUS (1) if the user was authenticated by the RADIUS server or LOCAL (2) if the user was authenticated by Dominion KX’s built-in user name database.
TERMINATE-CAUSE	If this is a STOP request, the reason the user was terminated. Either USER_REQUEST (1), LOST_SERVICE (3), SESSION_TIMEOUT (5), or ADMIN_RESET (6).

## Forced User Logoff

To manually log a user off a device, select that user in the user tree, right-click on the user icon, and select **Logoff User**.

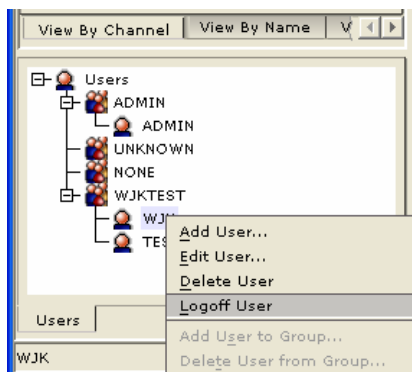


Figure 67 Logoff User Menu Option



## View KX Unit Event Log (Status)

On the **Setup** menu, click **Status** to view the device's Event Log. The device Status window appears, displaying events by date and time. Click **Export** and browse for a location to save the displayed log file to a text file. Click **Copy Log** to copy the display to your clipboard.

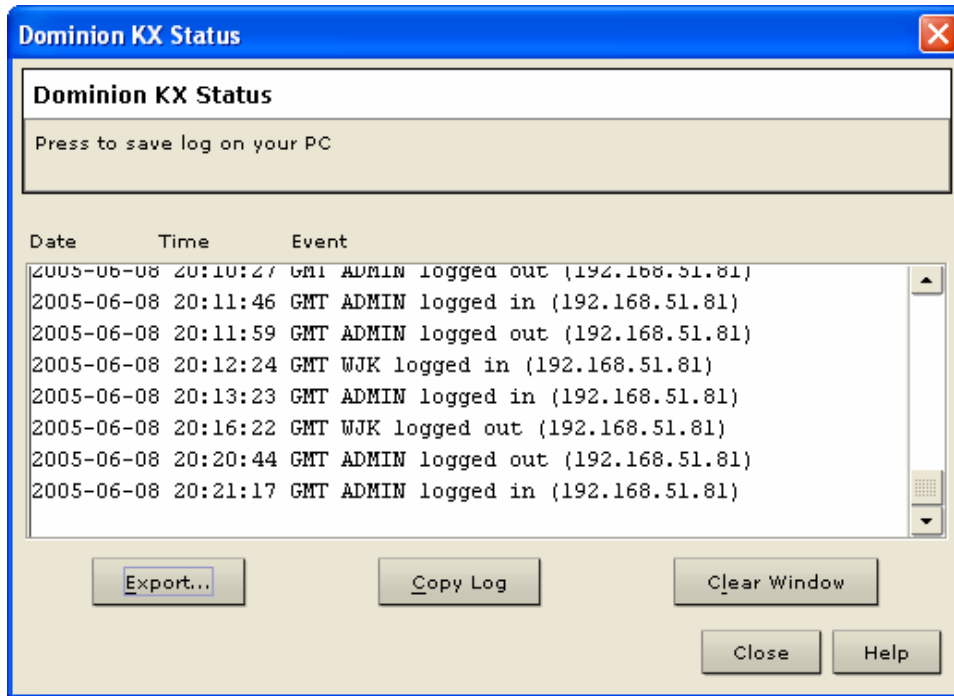


Figure 68 Status Log Window

## Rebooting the Device

When in KX Manager, on the **Setup** menu, click **Reboot Device** to reboot your device.

## Device Diagnostic Console

On the **Setup** menu, click **Diagnostics** to view a diagnostic console window from KX Manager (without having to launch RRC).

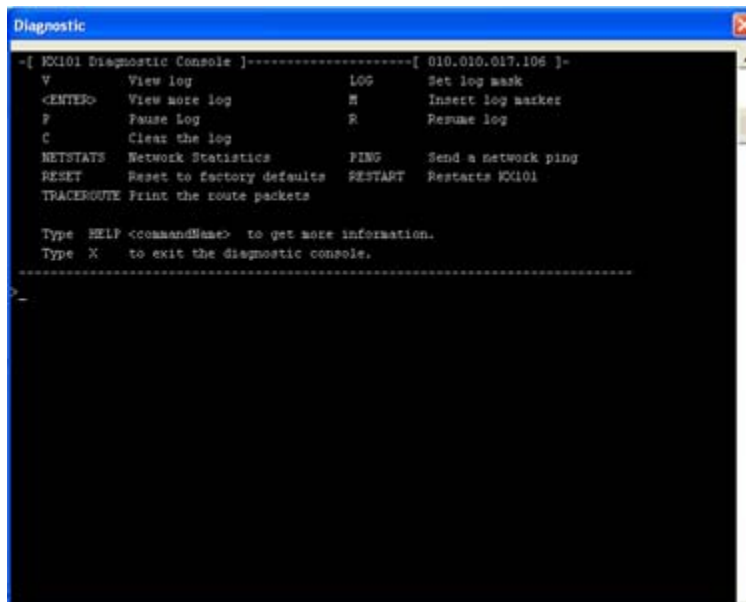


Figure 69 Device Diagnostic Window

To determine the Firmware Upgrade on the KX device, type **build info** at the prompt and press **Enter**. For releases KX 1.3 and higher, the Firmware Upgrade Version appears. This version number is in the same format as used on the Raritan.com firmware upgrade page.

## Device System Information

On the **Setup** menu, click **System Information** to view Model Type, Hardware Version, Firmware Version, Serial Number, and MAC Address of the device. The FPGA Version field is inactive.

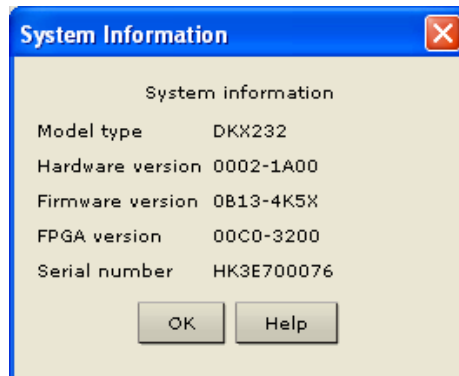


Figure 70 System Information Window (for Dominion KX)

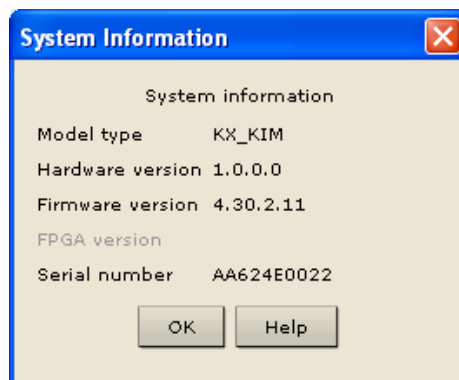


Figure 71 System Information Window (for KX101)

## Configuration Backup and Restore

On the **File** menu, click **Backup**, and then click **User-Group Information** to download User Group information. On the **File** menu, click **Backup**, and then click **Device Configuration** to download the complete device configuration to your local computer.

To restore User-Group information saved on your local computer, on the **File** menu, click **Restore**, and then click **User-Group Information**. To restore a Device configuration saved on your local computer, on the **File** menu, click **Restore**, and then click **Device Configuration**.

## Performance Settings

Use this window to set up the device's video data transfer and bandwidth parameters.

1. On the **Setup** menu, click **Configuration**, and then click **Performance**. The **Performance Settings** window appears.

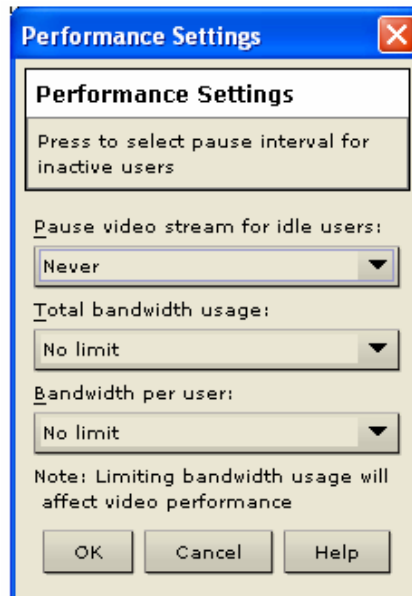


Figure 72 Performance Settings Window

2. **Pause Video Stream for Idle Users:** Click on the drop-down arrow to pause the flow of video data during periods of prolonged inactivity to prevent inactive users from needlessly consuming bandwidth. *Options:* Never / 5 / 15 / 30 / 60 / 120 minutes
3. **Total Bandwidth Usage:** Click on the drop-down arrow to set a maximum amount of bandwidth that can be consumed by this Dominion KX unit (global). The lower the bandwidth allowed, the slower the performance that may result. *Options:* No Limit / 10Mbps / 5Mbps / 2Mbps / 1Mbps / 512Kbps / 256Kbps / 128Kbps.
4. **Bandwidth per User:** Click on the drop-down arrow to set a maximum amount of bandwidth that can be consumed by each user logged onto this Dominion KX unit. *Options:* No Limit / 10Mbps / 5Mbps / 2Mbps / 1Mbps / 512Kbps / 256Kbps / 128Kbps.
5. Click **OK** to set Performance Settings or click **Cancel** to close the window.

## PC Properties

To view PC Properties, select a server in the server list and on the **Setup** menu, click **Properties**, and then click **PC** (or select a server in the server list, right-clicking on it, and click **Properties**).

- **Name:** This is the name given to the target in that channel. Administrators can change the name by typing a new one in this field. The target name can also be changed directly in the target list by clicking on the name once after it has been highlighted.
- **Type:** This describes what type of target is connected to this port. This value will always be CPU for a server target.
- **Status:** The availability of a target is shown in this field. **Available** indicates that no one is currently viewing the target, **Busy** indicates that a user is currently using the target, and **Unavailable** indicates that a configured target has been powered off or disconnected.
- **Power Strip** and **Outlet:** These fields are used for associating the selected target with a connected Remote Power Control Strip (please see the **Power Control** section in this chapter for additional information).

PC Properties: KVM Port

**Properties: PC**

Please enter name

Name: KVM Port      Type:      Status: Available

Power Strip	Outlet

OK    Cancel    Help

Figure 73 PC Properties Screen (shown on a Dominion KX with a Power Strip association)

---

**Note:** Power strip association is not available for KX101.

---

## Appendix A: Specifications

ITEM	DIMENSIONS (WxDxH)	WEIGHT (w/CABLE)	POWER
KX101	2.89"(W) x 4.04"(D) x 1.06"(H) 73.4mm(W) x 102.54mm(D) 27mm(H)	0.612lbs. (0.278kg.)	110/220V auto-switching (50/60 Hz European) 48VDC via PoE

### Remote Connection

Network: 10BASE-T, 100BASE-TX Ethernet  
 Protocols: TCP/IP, UDP, SNMP

### Raritan Remote Client Software

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

### KVM Input

Keyboard: PS/2 (via USB)

Mouse: PS/2 (via USB)

Video: VGA

Supported Resolutions:

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

### KVM Harness

Built-in KVM harness with PS/2 and USB pigtail attachments

### Local Console Port

RJ11 standard cord for serial communication



## Appendix B: KX101 Rack Mount

The KX101 unit can be mounted vertically or horizontally, facing the front or the rear, on either side of a server rack. Please use the brackets and screws included with the KX101 kit.

### AC-DC Adapter Clip Fitting

#### Identify Clip Type

---

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

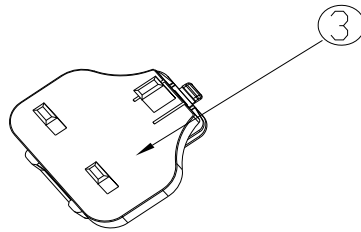
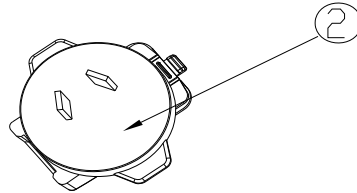
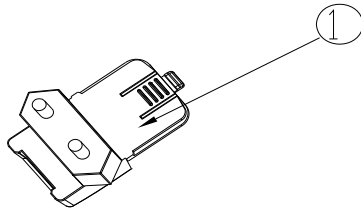


Figure 74 Power Adapter Clips

## Remove Attachment Cover from AC-DC Power Adapter

---

1. AC/DC Power Adaptor
2. Attachment Cover

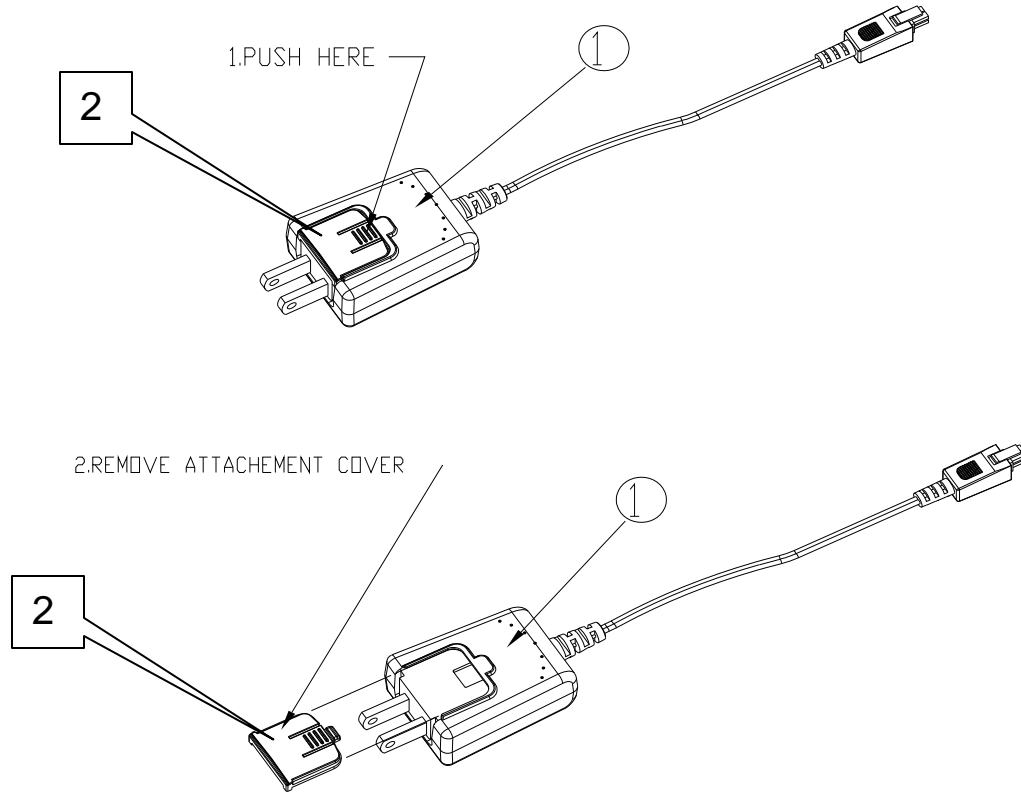


Figure 75 Attachment Cover on AC-DC Power Adapter



## Attach Clip to AC-DC Power Adaptor

---

1. Australian Clip
2. EU Clip
3. UK Clip
4. Power Adaptor

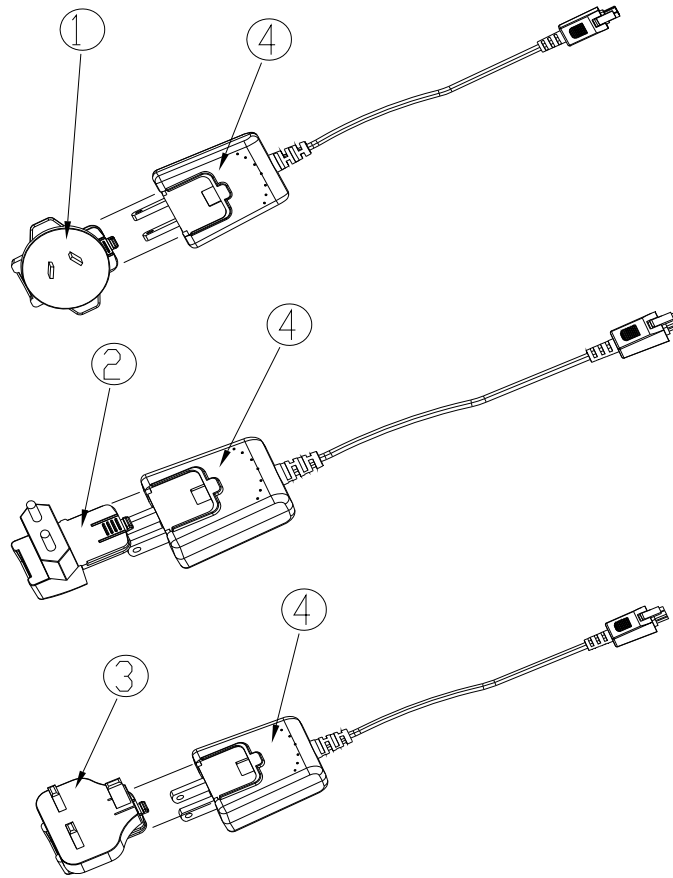


Figure 76 Clip Attachment

## Bracket Installation

1. KX101 unit
2. Right panel
3. Left panel
4. Screws

- Remove the screws from the KX101 unit.
- Slide the left and right panels off the KX101 unit.

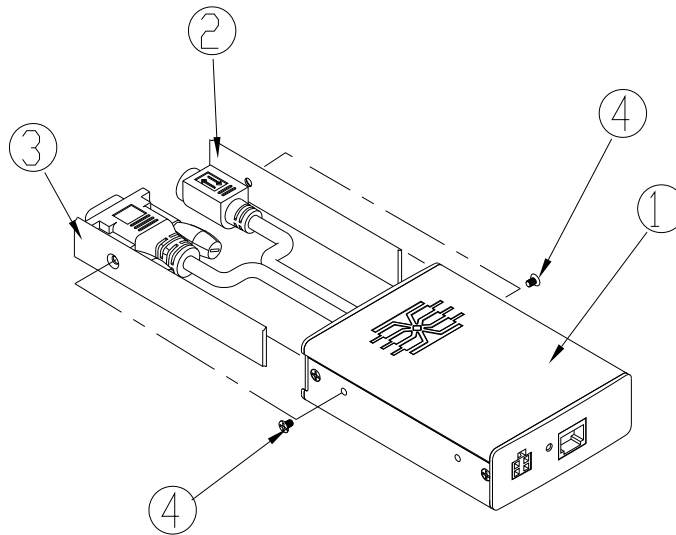
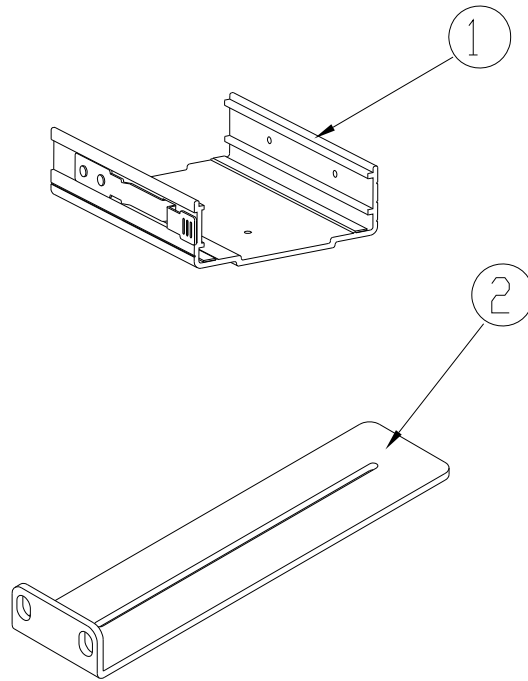


Figure 77 Panel Removal

## KX101 Bracket Parts

---

1. U Bracket
2. L Bracket



*Figure 78 Bracket Parts*

## Attach Brackets to KX101 for Horizontal Mount

1. KX101 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 KX101 unit into the U Bracket with the KVM harness facing towards the target. Pull and release the latch lever to lock the KX101 unit into the U Bracket.

The image below illustrates mounting the KX101 on the left. To mount the KX101 on the right, please follow these directions, but attach brackets to the **right** side of the KX101 unit.

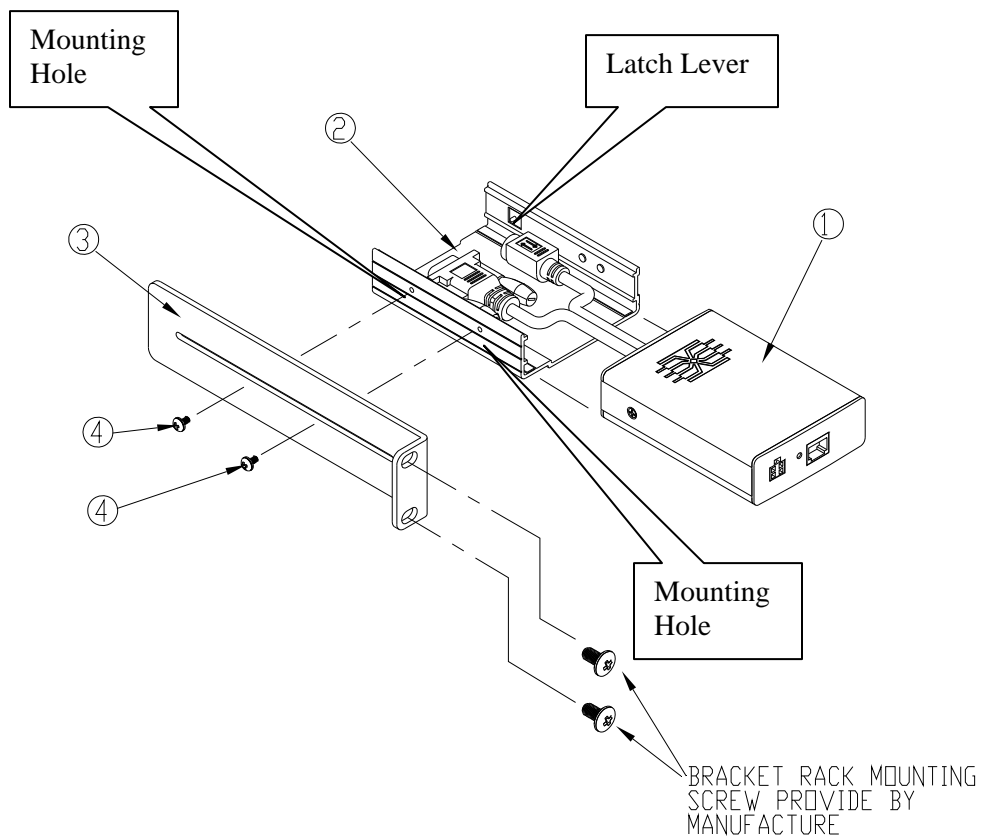


Figure 79 Attach Brackets to KX101 for Horizontal Mount

## Attach Brackets to KX101 for Vertical Mount

1. KX101 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 KX101 unit into the U Bracket with the KVM harness facing towards the target. Pull and release the latch lever to lock the KX101 unit into the U Bracket.

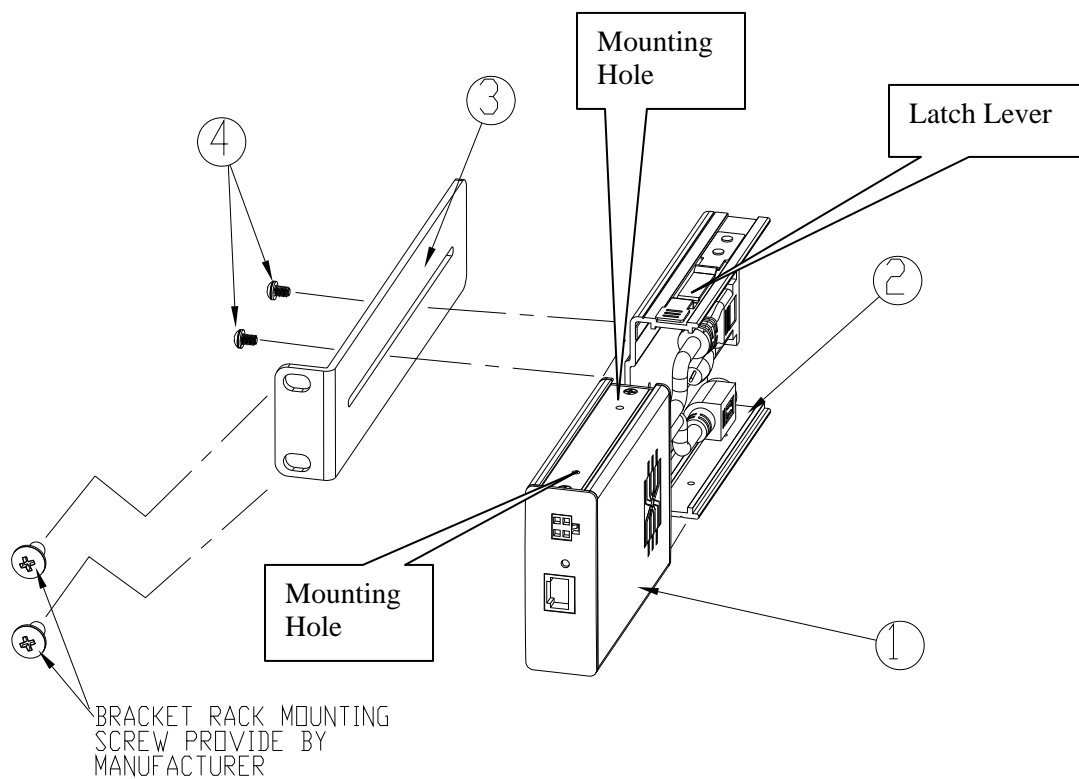


Figure 80 Attach Brackets to KX101 for Vertical Mount

## PS2 and USB Pigtails

1. PS2 Cable
2. USB Cable

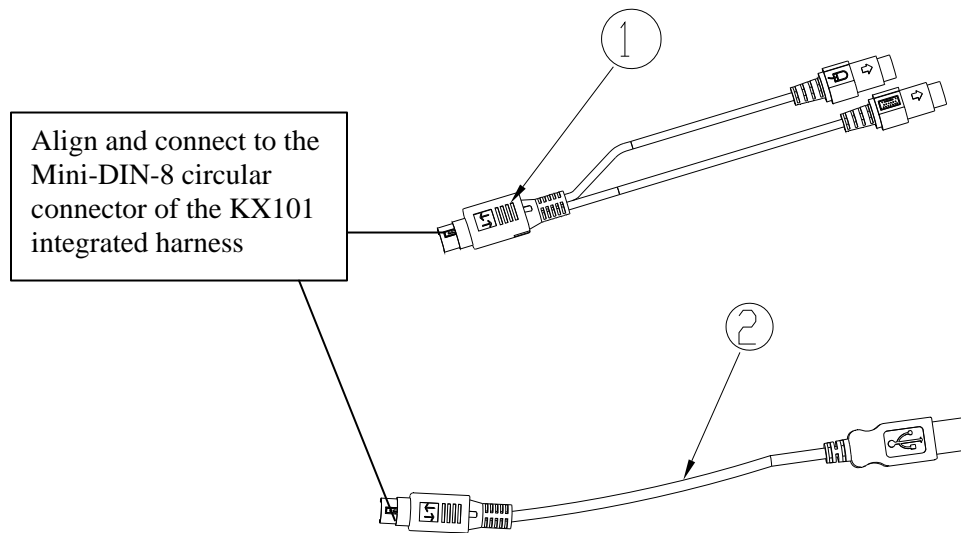


Figure 81 PS2 and USB Pigtails

## KX101 FAQs Online

Frequently Asked Questions for KX101 are now located online at [http://www.raritan.com/support/sup\\_faq.aspx](http://www.raritan.com/support/sup_faq.aspx).

255-62-4003