Dominion KX G1

User Guide

1.4.8

DKX116 DKX132, DKX216, DKX232, DKX416, DKX432, DKX464

DKX-0K-E
February 2008
255-80-6040

FCC Information

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

VCCI Information (Japan)

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

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

CE c UL us LISTED 1F61 I.T.E.

Contents

What's New in the User Guide

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

- Red Hat 4/Red Hat 9/SUSE Linux 10.1
- Making Linux Settings Permanent
- Setup Preparation

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

Safety Guidelines

To avoid potentially fatal shock hazard and possible damage to Raritan equipment:

- Do not use a 2-wire power cord in any product configuration.
- Test AC outlets at your computer and monitor for proper polarity and grounding.
- Use only with grounded outlets at both the computer and monitor. When using a backup UPS, power the computer, monitor, and device off the supply.

Rack Mount Safety Guidelines

For Raritan products that require rack mounting, follow these precautions:

- Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the devices (see ***Appendix A: Specifications*** (see "Specifications" on page 217) for additional information).
- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly to the branch circuit, especially supply connections such as power strips (other than direct connections).

Chapter 1 Introduction

In This Chapter

Dominion KX Overview

The Dominion KX is an enterprise-class, secure, digital KVM switch that provides BIOS-level access and control of 64 servers from anywhere in the world via a web browser. At the rack, The Dominion KX provides BIOS-level control of up to 64 servers and other IT devices from a single keyboard, monitor, and mouse. The Dominion KX's integrated remote access capabilities provide the same BIOS-level control of your servers, from anywhere in the world, via a web browser.

The Dominion KX is easily installed using standard UTP (Cat 5/5e/6) cabling. Its advanced features include 128-bit encryption, remote power control, dual Ethernet, LDAP, RADIUS, Active Directory, syslog integration, and web management. These features enable you to deliver higher uptime, better productivity, and bulletproof security - at any time from anywhere.

For larger data centers and enterprises, multiple Dominion KX units (along with Dominion SX units for remote serial console access and Dominion KSX for remote/branch office management) can be integrated into a single logical solution via Raritan's CommandCenter Secure Gateway (CC-SG).

The Dominion KX series includes KX132 and KX464 models. The Dominion KX132 offers an economical alternative with the same KX reliability. The KX464 is a 64-port digital KVM switch that offers a dual power option for added reliability. In addition, intelligent mouse synchronization and SNMP management are also available with these devices.

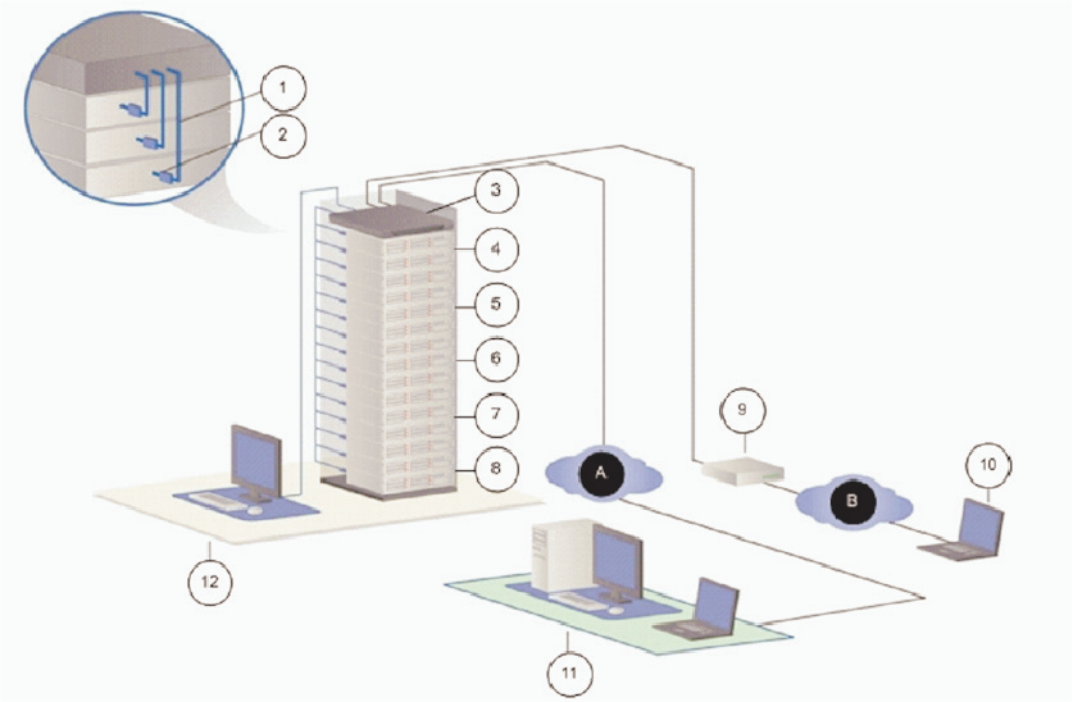
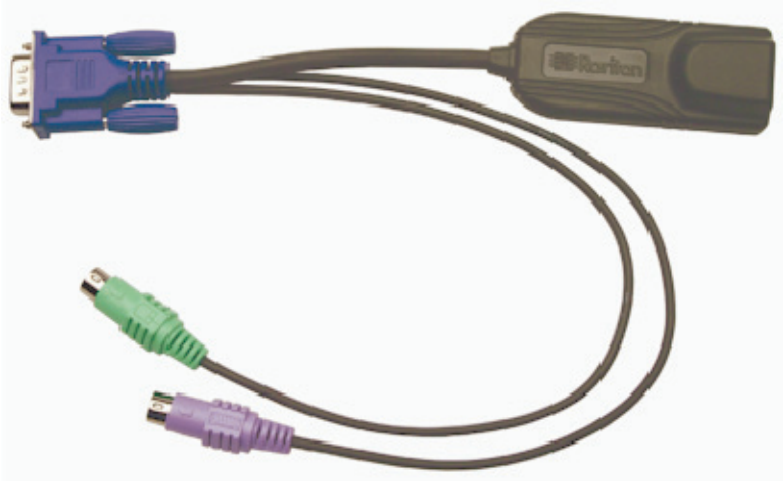


Diagram key			
1	UTP (Cat5/5e/6) Server Cabling	8	Sun Solaris
2	Computer Interface Module	9	External Modem (optional)
3	Dominion KX	10	Modem Access
4	WinXP	11	Remote Network Access
5	Win2000	12	Local Rack Access
6	Linux/UNIX	A	LAN
7	Novell	B	PSTN

Product Photos



Product Features

Hardware

- 1U or 2U rack-mountable (brackets included)
- Dual power with failover (with the KX464)
- Dual-failover Ethernet ports
- 16, 32, or 64 (on KX464) server ports
- Multiple user capacity
- UTP (Cat5/5e/6) server cabling
- Dual failover 10/100 LAN
- Modem-ready via external modem port
- FLASH upgradeable
- Auto-switching power supply
- Local user port for rack access
  - PS/2 and USB keyboard/mouse ports
  - Fully concurrent with remote users
  - Onscreen display
- Centralized access security
- Integrated power control
- LED indicators for power, network activity, and remote user status
- Integrated KVM over IP remote access
- Cross-platform server support

Software

- Plug and play device
- Web-based access and management
- Intuitive graphical user interface
- Integration with Raritan's CommandCenter Secure Gateway (CC-SG)
- High-color (15-bit+) palette support
- 128-bit encryption of complete KVM signal, including video
- LDAP, RADIUS, Active Directory, or Internal Authentication
- DHCP or fixed IP addressing
- SNMP management
- Intelligent mouse synchronization
- CC UnManage (via the Dominion KX Manager)

Terminology

This manual uses the following terms for components of a typical Dominion KX configuration. Refer to the diagram for clarification, if needed.

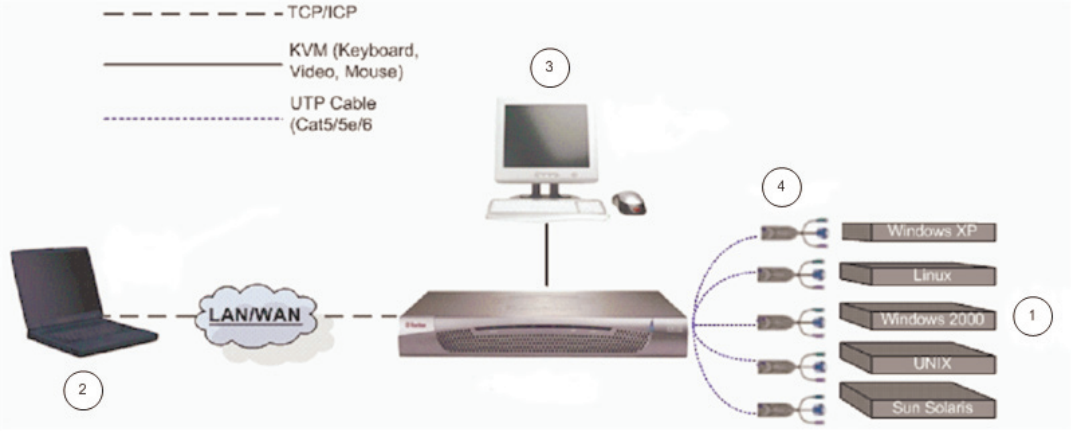


Diagram key		
1	Target servers	Servers with graphical video cards and user interfaces (for example., Windows, Linux, Solaris, etc.) to be accessed remotely via the Dominion KX.
2	Remote PC	A networked computer used to access and control target devices connected to the Dominion KX.
3	Local access console	An optional user console, consisting of a keyboard, mouse, and multi-sync VGA monitor, that is directly attached to the Dominion KX to control target servers locally (directly at the rack, not through the network).
4	CIM (Computer Interface Modules)	Server dongles (Raritan P/N DCIM-xxxx) that connect to each target server. Available for PS/2, Sun, USB, and Sun USB keyboards and mouse ports.

Important Information

Default IP Address

Dominion KX default IP address	
Default IP address	192.168.0.192

Login

Dominion KX defaults	
Default login	admin
Default password	raritan (passwords are case sensitive; enter the default password using all lower case)
Default user privileges	Administrative

To ensure security, change the default password as soon as possible. For backup and business continuity purposes, Raritan suggests that customers create a backup administrator login and keep the password in a secure location.

Service Pack

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

User Guide Scope

This user guide applies to Dominion KX devices using firmware 1.4.8, which operates on all Dominion models: DKX116, DKX1342, DKX216, DKX232, DKX416, DKX432, and DKX64.

To determine the firmware upgrade version on an existing KX device, choose System Information on the Setup menu in KX Manager or press the F8 key on your keyboard. To upgrade your firmware, go to the Support > Firmware Upgrades > Dominion KX page on the Raritan website (***http://www.raritan.com*** http://www.raritan.com).

Supported Browsers

The Dominion KX supports the following browsers:

- Internet Explorer 6
- Mozilla 1.7
- Safari 2.0 or later (Mac OS 10.4.9 or later)
- Netscape 7.2
- Firefox 1.0 or later

Note: Netscape 8 has an option that allows you to change the rendering engine. When Firefox is selected as the rendering engine from Netscape, the Multi-Platform Client (MPC) is used to access targets. When Internet Explorer is selected as the rendering engine from Netscape, the Raritan Remote Client (RRC) is used to access targets. See ***Multi-Platform Client and Raritan Remote Client*** (on page 26) for more information on using RRC and MPC.

Supported Paragon CIMs

The Dominion KX version 1.4 and higher supports the following CIMs:

- DCIM-PS2 for PS/2 KB/MS
- DCIM-SUN for SUN KB/MS
- DCIM-USBG2 for USB KB/MS (not Sun)
- DCIM-USBG2 for SUN USB KB/MS
- P2CIM-PWR for power strip control
- UUSBPD
- P2CIM-PS2
- P2CIM-SUN
- P2CIM-USB
- P2CIM-SUSB
- UKVMPD
- USKVMPD

Note: There is a small switch on the DCIM-USBG2 that should be set to the S position for use with SUN Solaris servers.

Supported Keyboard and Mouse Devices

The Dominion KX supports the following on local console devices:

- USB keyboard and USB mouse (two distinct connectors)
- PS/2 keyboard and PS/2 mouse (two distinct connectors)
- PS/2 keyboard with a USB mouse
- USB keyboard with a PS/2 mouse
- Combo USB keyboard/mouse with one USB plug
- USB hubs (up to 3, in any combination)
- PS/2 to USB adapters (in most cases)
- USB to PS/2 adapters (in most cases)
- Keyboards that allow additional USB keyboards, mice, and/or hubs to be plugged into the keyboard itself (keyboard functions as a hub)
- Various keyboard trays and drawers

Package Contents

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

Amount included	Item
1	Dominion KX unit
1	Dominion KX printed quick setup guide
1	Raritan user guide CD-ROM
1	Rackmount kit
1	AC power cord
1	Cat5 network cable
1	Cat5 network crossover cable
1	Set of 4 rubber feet (for desktop use)

Chapter 2 Installation

In This Chapter

Configuring Target Servers

Before installing the Dominion KX, you must configure any target servers that will be accessed via the Dominion KX to ensure optimum performance. Note that the configuration requirements outlined in this section apply only to target servers, not to the client workstations (remote PCs) that are used to access the Dominion KX remotely.

Server Video Resolution

Ensure that each target server's video resolution and refresh rate is supported by the Dominion KX and that the signal is noninterlaced. Dominion KX supports the following video resolutions:

Resolutions		
640x480 @ 60Hz	800x600 @ 56Hz	1024x768 @ 60Hz
640x480 @ 72Hz	800x600 @ 60Hz	1024x768 @ 70Hz
640x480 @ 75Hz	800x600 @ 72Hz	1024x768 @ 75Hz
640x480 @ 85Hz	800x600 @ 75Hz	1024x768 @ 85Hz
720x400 @ 70Hz	800x600 @ 85Hz	1152x864 @ 60Hz
720x400 @ 85Hz		1152x864 @ 70Hz
		1152x864 @ 75Hz
		1280x960 @ 60Hz
		1280x1024 @ 60Hz

Desktop Background

For optimal bandwidth efficiency and video performance, target servers running graphical user interfaces such as Windows, Linux, X-Windows, Solaris, and KDE should be configured with desktop backgrounds set to a predominantly solid, plain, light-colored graphic. The desktop background need not be completely solid; but desktop backgrounds featuring photos or complex gradients should be avoided.

Mouse and Video Settings

Mouse Modes

The Dominion KX operates in Standard Mouse mode by default, which requires that acceleration be disabled. However, depending on your operating system, you can choose to work in Intelligent Mouse mode. In either mode, mouse parameters must be set to specific values (described in this user guide). See ***Single Mouse Mode/Dual Mouse Mode*** (on page 99) for more information.

Note: Although Absolute Mouse mode appears on the Mouse menu, it is disabled at this time.

Note that mouse configurations will vary on different target operating systems system. Consult your operating system guidelines for further details.

Windows XP/Windows 2003 Mouse 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 > Pointer Options. Disable transition effects in Control Panel > Display > Appearance > Effects.

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

Windows XP and 2000 login screens revert to preset mouse parameters that differ from those suggested for optimal Dominion KX performance. As a result, mouse synchronization may not be optimal at these screens.

If you are comfortable adjusting the registry on Windows target servers, you can obtain better Dominion KX 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.

Important: Only the default, Standard mouse mode works with these operating systems.

Windows 2000/ME Mouse Settings

On target servers running Microsoft Windows 2000/ME, 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. Disable transition effects in Control Panel > Display > Effects.

Windows 95/98/NT Mouse Settings

On target servers running Microsoft Windows 95/98/NT, set the mouse motion speed to the slowest setting in Control Panel > Mouse > Motion. Disable window, menu, and list animation in Control Panel > Display > Effects.

Linux Mouse Settings

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

Ensure that each target server running Linux is using a resolution supported by the Dominion KX 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:

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

Note: In many Linux graphical environments, the command <Ctrl+Alt+ + (plus key)> will change the video resolution, scrolling through all available resolutions that remain enabled in the XF86Config file.

Red Hat 4/Red Hat 9/SUSE Linux 10.1

On target servers running Linux graphical interfaces, follow these steps to configure mouse settings:

1. Choose Main Menu > Preferences > Mouse. The Mouse Preferences dialog appears.
2. Click to select the Motion tab.
3. Within the Speed group, set the Acceleration slider to the exact center position.
4. Within the Speed group, set the Sensitivity towards low.
5. Within the Drag & Drop group, set the Threshold towards small.
6. Close the Mouse Preferences dialog.

Making Linux Settings Permanent

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

➢ ***To add a prompt:***

1. Choose Main Menu > Preferences > More Preferences > Sessions. The Sessions dialog appears.
2. On the Session Options tab, check the "Prompt on logout" checkbox and click OK. This option prompts you to save your current session when you logout.
3. Upon logging out, check the "Save current setup" option.
4. Click OK.

➢ ***To remove a prompt:***

1. Choose Main Menu > Preferences > More Preferences > Sessions. The Session dialog appears.
2. On the Session Options tab, deselect the "Prompt on logout" checkbox.
3. Check the "Automatically save changes to the session" checkbox and click OK. This option automatically saves your current session when you log out.

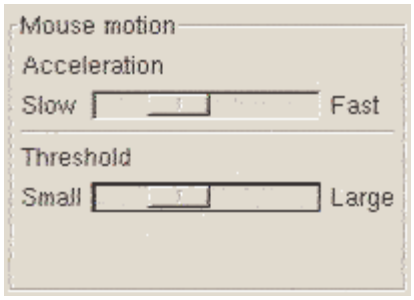
Note: Mouse settings are associated with the user account (user name and password). The mouse settings will be fixed as long as the same user account is used (even if the user logs out or reboots the machine).

Sun Solaris Video and Mouse Settings

Sun Solaris Mouse Settings

On target servers running the Solaris operating system, set the mouse acceleration value to exactly 1 and the threshold value to exactly 1.

This can be performed from the graphical user interface or with the following command line: `xset mouse a t` where `a` is the acceleration and `t` is the threshold.



➢ ***To configure the mouse settings for Sun Solaris 10.1:***

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

Sun Solaris Video Settings

All target servers must be configured to one of the display resolutions supported by the Dominion KX (see ***Server Video Resolution*** (on page 11)). The most popular supported resolutions for Sun machines are:

- 1024 x 768 @ 60 Hz
- 1024 x 768 @ 70 Hz
- 1024 x 768 @ 75 Hz
- 1024 x 768 @ 85 Hz
- 1152 x 900 @ 66 Hz
- 1152 x 900 @ 76 Hz
- 1280 x 1024 @ 60 Hz

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

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

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

You may also contact your Raritan representative to purchase a video output adapter. 13W3 Suns with composite sync output require an APSSUN II Guardian converter for use with the Dominion KX. HD15 Suns with composite sync output require the 1396C converter to convert from HD15 to 13W3 and an APSSUN II Guardian converter to support composite sync. HD15 Suns with separate sync output require an APKMSUN Guardian converter for use with the Dominion KX.

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

Apple Macintosh Mouse Settings

For target servers running an Apple Macintosh operating system, no specific mouse setting is required. However, when using the Dominion KX to access and control your target server, you must set Multi-Platform Client (MPC) to use Single Cursor mode (see ***Single Mouse Mode/Dual Mouse Mode*** (on page 99) for information on working with Single Cursor mode).

Single Cursor mode for Apple Macintosh target servers is supported using MPC. Single button mice are also supported on Mac OS 10.4.x and later clients when MPC is launched in a browser and as a standalone application . Hold down the Ctrl key and click with the mouse to emulate right clicking in MPC.

The standalone version of MPC supports Apple Macintosh modem connections as well.

Note: See the Raritan Multi-Platform Client and Raritan Remote Client User Guide, available on Raritan's website in the Support section or on the Raritan user guides & quick setup guides CD ROM included with your Dominion KX shipment for details on installing and operating MPC and RRC.

Note: If both non-MAC and MAC targets are connected, it is strongly recommended to use a 2-button mouse on a MAC target to avoid confusion when switching between MAC and non-MAC targets.

IBM AIX Mouse Settings

For target servers running the IBM-AIX UNIX operating system, follow these steps to make mouse settings permanent:

1. Go to Style Manager.
2. In Style Manager dialog, choose the Mouse option.
3. In the Mouse dialog, use the sliders to set the Acceleration setting to 1.0 and the Threshold to 1.0.
4. Click OK.

Configuring Network Firewall Settings

If you wish to access the Dominion KX through a network firewall, your firewall must allow communication on TCP Port 5000. The Dominion KX can also be configured to use a different TCP port of your designation (see ***Network Configuration*** (on page 150) for additional information).

Optional: Take advantage of the Dominion KX's web-access capabilities. To do this, the firewall must also allow inbound communication on TCP Port 443 - the standard TCP port for HTTPS communication.

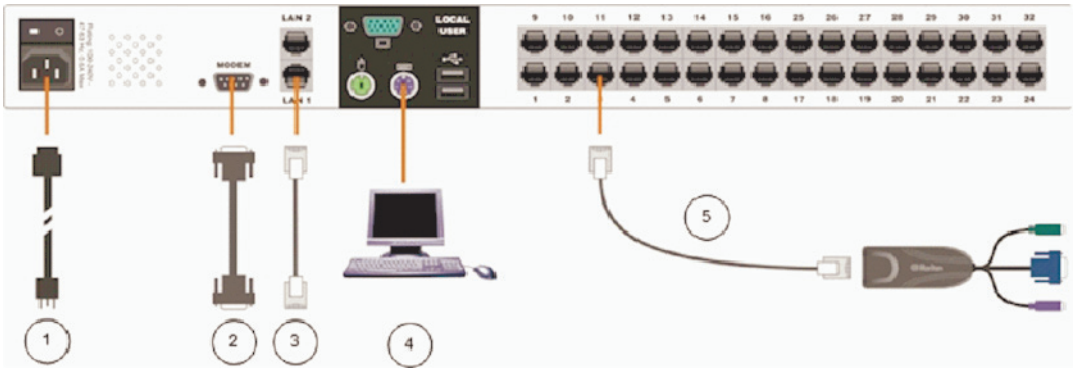
To take advantage of the Dominion KX's automatic redirection of HTTP requests to HTTPS (for example, so users may type the more common http:// instead of https://), the firewall must also allow inbound communication on TCP Port 80 - the standard TCP port for HTTP communication.

Note: Depending on hardware status, firewall ports may require different settings. Refer to the table:

Port	Old device	New device
5000 UDP	Can be used for discovery	Will be used for discovery
5002 UDP	Can be used for discovery	Not supported
5000 TCP	Can be used for connecting to the device	Will be used for connecting to the device
5001 TCP	Can be used for connecting to the device	Not supported

Physical Connections

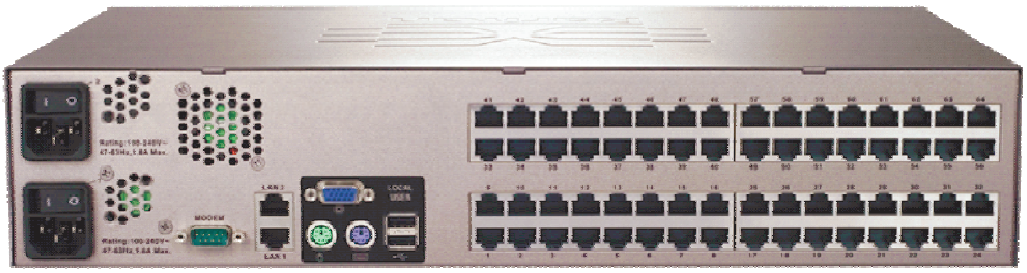
The numbers in the diagram correspond to the topics in this section of the user guide that describe the connection.



1. AC Power Line

Attach the included AC power cord to the Dominion KX and plug it into an AC power outlet.

If you are installing a KX464 and want dual power failover protection, attach the second included AC power cord and plug it into a different power source.



2. Modem Port (optional)

The Dominion KX features a dedicated modem port for remote access even when the LAN/WAN is unavailable. Using a straight-through serial (RS-232) cable, connect an external serial modem to the port labeled MODEM on the back of the Dominion KX (see ***Specifications*** (on page 217) for a list of certified modems and ***Administrative Functions*** (on page 146) for additional information on modem functions).

Use both network ports only if you want to use one as a failover port; using both ports is not mandatory. As with failover power supply, plug the second serial cable into a different switch than the first cable.

Note: Raritan recommends configuring the modem by enabling the CD (carrier detect) setting.

3. Network Ports

The Dominion KX provides two Ethernet ports for failover purposes (not for load-balancing). By default, only LAN1 is active and automatic failover is disabled. In the event that the Dominion KX internal network interface or the network switch to which it is connected becomes unavailable, the port labeled LAN2 will become enabled and will use the same IP address.

Connect a standard Ethernet cable (included) from the network port labeled LAN1 to an Ethernet switch, hub, or router. To make use of the Dominion KX's Ethernet failover capabilities, you must also connect a standard Ethernet cable from the network port labeled LAN2 to an Ethernet switch, hub, or router and then Enable Automatic Failover on the Network Configuration page in KX Manager.

4. Local Access Console Ports (optional)

For convenient access to target servers while at the rack, use the Dominion KX's Local Access Console ports. Attach a multisync VGA monitor, mouse, and keyboard to the ports labeled Local User using either a PS/2 keyboard and mouse, or a USB keyboard and mouse.

The USB keyboard and mouse ports are to be used only for keyboard and mouse access. Other USB devices such as external drives, scanners, etc. should not be connected to these ports.

5. Server Ports

The Dominion KX uses standard UTP cabling (Cat5/5e/6) to connect to each target server. See ***Appendix A: Specifications*** (see "Specifications" on page 217) for additional information.

To connect a target server to the Dominion KX, use the appropriate Computer Interface Module (CIM):

- DCIM-PS2
- DCIM-SUN
- DCIM-USB
- DCIM-SUSB
- PS/2 keyboard/mouse
- Sun keyboard/mouse
- USB keyboard/mouse
- USB keyboard/mouse for Sun Microsystems servers

Attach the HD15 video connector of your CIM to the video card of your target server. Ensure that your target server's video has already been configured to a supported resolution and refresh rate. For Sun servers, also ensure that your target server's video card has been set to output standard VGA (H-and-V sync) and not composite sync.

Attach the keyboard/mouse connector of your CIM to the corresponding ports of your target server. Then, using a standard straight-through UTP (Cat5/5e/6) cable, connect the CIM to an empty server port on the back of your Dominion KX unit.

Note: Other CIMs supported by DKX version 1.3 and higher include: P2CIM-PS2, P2CIM-SUN, P2CIM-USB, P2CIM-SUSB, UKVMPD, USKVMPD, UUSBPD, and P2CIM-PWR (for power strip control).

When using a DCIM-SUSB, follow these steps to change keyboard layout code:

1. Open a Text Editor dialog on the Sun workstation.
2. Ensure that the NUM LOCK key is active and press the left Ctrl key and the DEL key on your Keypad. The Caps Lock LED starts to blink, which indicates that the CIM is in Layout Code Change mode.
3. The text window displays the following: Raritan Computer, Inc. Current keyboard layout code = 22h (US5 Unix).
4. Type the layout code desired (for example, 31 for Japanese keyboard).

5. Press Enter.
6. Shut down the unit and power ON once again so that the DCIM-SUSB performs a reset (power cycle).
7. Use MPC or C/MPC to switch in again and press keys to verify all character is correct.

Initial Configuration

IMPORTANT: In some environments, the default 10/100 Mb autonegotiation does not properly set the network parameters, leading to network issues. For an example, visit http://www.cisco.com/warp/public/473/3.html.

In these cases, setting the Dominion KX to 100 Mbps/Full Duplex (or whatever is appropriate to your network) addresses the issue.

To set this parameter, on the Network Settings page, select Autonegotiate and set the values appropriate to your network.

Note to CC-SG Users

If you are using the Dominion KX in a CC-SG configuration, perform the installation steps as outlined and, when finished, consult the CommandCenter Secure Gateway User Guide, Administrator Guide, or Deployment Guide to proceed. These guides can be found on the Raritan website.

Assigning an IP Address

1. Power on the Dominion KX via the power switch on the back of the unit. Wait approximately 45 seconds as the Dominion KX boots.
2. After the KX unit boots, the onscreen display (local console) appears on the monitor attached to the Dominion KX's Local Access Console. Log in with the default user name/password of admin/raritan and press Enter.
3. Press the F5 key on your keyboard to activate the Administrative menu.
4. Choose Option 3, Network Settings, and press Enter.
5. Specify TCP/IP parameters for your Dominion KX unit: IP address, subnet mask, and default gateway. When finished, press the S key to save the settings. The Dominion KX unit will automatically reboot.

6. Connect one end of a straight-through Ethernet cable (included) to the port labeled LAN1 on the rear panel of the Dominion KX, and connect the other end to a network switch or router. Your Dominion KX unit is now network accessible.

Note: If two Dominion KX units are assigned the same IP address, an IP conflict results. A Raritan Remote Console attempting to connect to one of the units may get a "Bad Parameter" message. This is because the RRC discovers devices and maintains a list of discovered devices using the IP address of the device as the key. The device ID is also stored with the key. If another KX is discovered with the same IP address, the RRC will not know there an IP conflict. When the RRC starts communicating with the second device, it uses the device ID from the first device. As a result, the second device issues the Bad Parameter message.

Connecting To and Naming Target Servers

Connect one end of a standard, straight-through UTP cable (Cat5/5e/6) to an unoccupied server port and connect the other end to the RJ45 port on a Dominion KX Computer Interface Module (CIM): DCIM-PS2 (PS/2 ports), DCIM-USBG2 (USB ports and Sun servers), or DCIM-SUN (Sun ports with HD15 video).

Note: There is a small switch on the DCIM-USBG2 that should be set to the S position for use with Sun Solaris servers.

1. Connect the remaining ports on the CIM to the corresponding KVM ports of the server that you wish to manage using the Dominion KX. Continue connecting to all servers that you wish to manage using the Dominion KX.
2. On the local access console, log in with the default user name/password of admin/raritan.
3. Press the F5 key to activate the Administrative menu and choose Option 5, Channel Configuration.
4. Choose a server port to rename and press the Enter key. When the cursor changes to a green color, assign a name (up to 20 characters, alphanumeric, no symbols allowed) to identify the server connected to that port.
5. Press Enter to complete the change.
6. Press Esc to exit the menu.

Changing the Default Password

1. Find and log in to any workstation with (a) network connectivity to your Dominion KX unit, and (b) Java Runtime Environment v1.4.2_2 or higher installed (Java Runtime Environment is available at http://java.sun.com/).
2. Launch a web browser such as Internet Explorer or Mozilla.
3. If you are using Internet Explorer (IE) type the following URL: *http://IP-ADDRESS/admin*, where IP-ADDRESS is the IP address that you assigned to your Dominion KX unit.
4. The Dominion KX remote management tool, Dominion KX Manager, will launch. Log in with the default username and password (admin/raritan).
5. In the User Navigation tree in the left panel of the page, select the Admin User icon.
6. Right-click on the Admin User icon and choose Edit User from the shortcut menu.
7. Type a new password in the Password field. Retype the password in the Confirm Password field. Passwords consist of twenty (20) English alphanumeric characters and the following symbols: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.
8. Click OK to save User properties.

The Default Password can also be changed from Raritan Multi-Platform Client and Raritan Remote Client (MPC and RRC). See ***Changing a Password*** (on page 127)in the ***Multi-Platform Client and Raritan Remote Client*** (on page 26) section of this guide.

Upgrading Device Firmware

You will upgrade the Dominion KX's firmware using MPC or RRC. See *Upgrading Device Firmware* (on page 126) in the *Multi-Platform Client and Raritan Remote Client* (on page 26) section of this guide for more information.

Note: When you upgrade a device, the device goes into a Maintenance mode. All sessions are disconnected and the device can execute only certain required software components. This allows the system to be in a clean, well understood state so that firmware update operations can occur reliably.

Updating User Passwords

After upgrading your firmware (see *Upgrading Device Firmware* (on page 126)), the Change Password dialog automatically appears. Fill in new password information. You are also able to manually change a user's password at any time. See *Changing a Password* (on page 127).

Multi-Platform Client and Raritan Remote Client

Requirements and Installation

MPC Requirements and Installation Instructions

Note to CC-SG Users

If you are using Dominion KX II in a CC-SG configuration, do not use the CC-SG proxy mode if you are also planning to use the Multi-Platform Client (MPC).

MPC Minimum System Requirements

The minimum system requirements for the Multi-Platform Client are:

- CPU Speed: 1.0 GHz
- RAM: 512 Mbytes

Note: Running the client software on system configurations below either of these specifications may impact performance and result in errors.

MPC Supported Browsers

MPC supports the following browsers:

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

Raritan Multi-Platform Client (MPC) Supported Operating Systems

When launched as a web applet or as a standalone application, MPC allows you to reach target servers via different Raritan Dominion devices and IP Reach models.

Raritan MPC is compatible with the following platforms:

- Windows XP
- Windows 2000 SP4
- Windows Vista
- Red Hat Linux® 9.0
- Red Hat Enterprise Workstation 3.0 and 4.0
- SUSE Linux Professional 9.2 and 10
- Fedora Core 5 and above
- Mac®
- Solaris™

Launching MPC from a Web Browser

Important: Regardless of the browser you use, you must allow pop-ups from the Dominion device's IP address in order to open MPC.

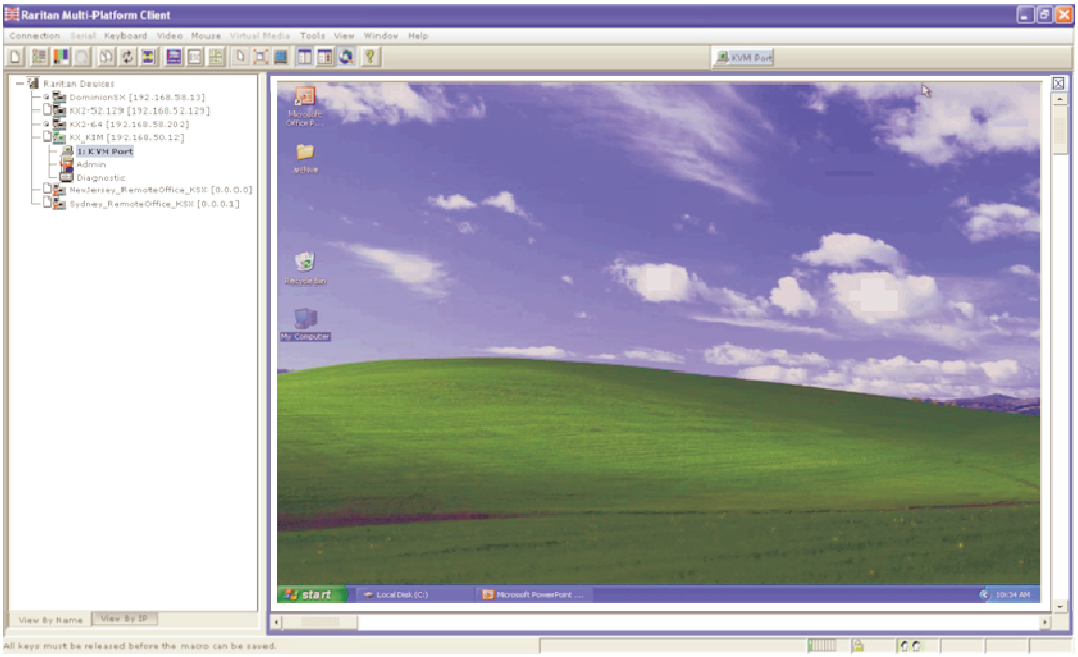
1. To open MPC from a client running any ***supported browser*** (see "MPC Supported Browsers" on page 27), type *http://IP-ADDRESS/mpc* into the address line, where IP-ADDRESS is the IP address of your Raritan device. MPC will open in a new window. This window will not contain a menu bar, toolbar, scroll bar, or address bar. Work in this window and toggle to other open windows using the Alt+Tab command.

   Note: The Alt+Tab command will toggle between windows only on the local system.

   When MPC opens, the Raritan devices that were automatically detected and which are found on your subnet are displayed in the Navigator in tree format.

2. If your device is not listed by name in the navigator, add it manually:
   a. Choose Connection > New Profile. The Add Connection window opens.
   b. In the Add Connection window, type a device Description, specify a Connection Type, add the device IP Address, and click OK. These specifications can be edited later.
3. In the Navigator panel on the left of the page, double-click on the icon that corresponds to your Raritan device to connect to it.

Note: Depending on your browser and browser security settings, you may see various security and certificate check and warning messages. It is necessary to accept the options in order to open MPC.



Installing and Opening Standalone MPC

Raritan recommends that you open only one standalone MPC session at a time. Opening more than one standalone MPC session on the same client at the same time may cause performance problems and system errors.

Note: Note that the installer file names and the install directories/folder paths that are documented in the device user guides may differ slightly from what is outlined in this guide.

Important: MPC modem connectivity is supported on Windows, Linux, and Sun Solaris but not Macintosh. When working in Windows, use Standalone MPC.

You must have the MPC JAR file to install MPC for any of these operating systems.

1. Download the installation file, MPC-installer.jar from the Raritan website on the Support - Firmware Upgrades page (http://www.raritan.com/support/firmwareupgrades). Click on Dominion Family and scroll to the Standalone Multi-Platform Client link.
2. If copying MPC-installer.jar from a known location, double-click on the file to start installation.

Windows

Checking JRE Version in Windows

1. Do one of the following to check the JRE version in Windows:
   - Determine your version of the JRE from the Java website: http://www.java.com/en/download/help/testvm.xml.
   - Click on the Windows Start button at the bottom left of your page and click Control Panel.

   Tip: In the upper left corner of the page, you may see a panel named Control Panel with the option Switch to Classic View or Switch to Category View. For easier viewing, opt for Classic View.

   a. Search the Control Panel files for a Java icon. When you locate the Java icon, double-click on it to open the Java Control panel. Click on the General tab and then click on the About button to check the current Java Runtime Environment (JRE).

b. If the JRE is version 1.4.2_05 or later, proceed with the MPC Installation. If the Java icon does not exist in the Control Panel or if the JRE version is prior to 1.4.2_05, go to the Sun Microsystems website at http://java.sun.com/products/ to download the latest version of JRE.

2. For future Java access and to automatically open it, set your path to the Java executable.

   a. Right-click on the My Computer icon on your desktop and click Properties.

   b. Click on the Advanced tab and then click "Environment variables".

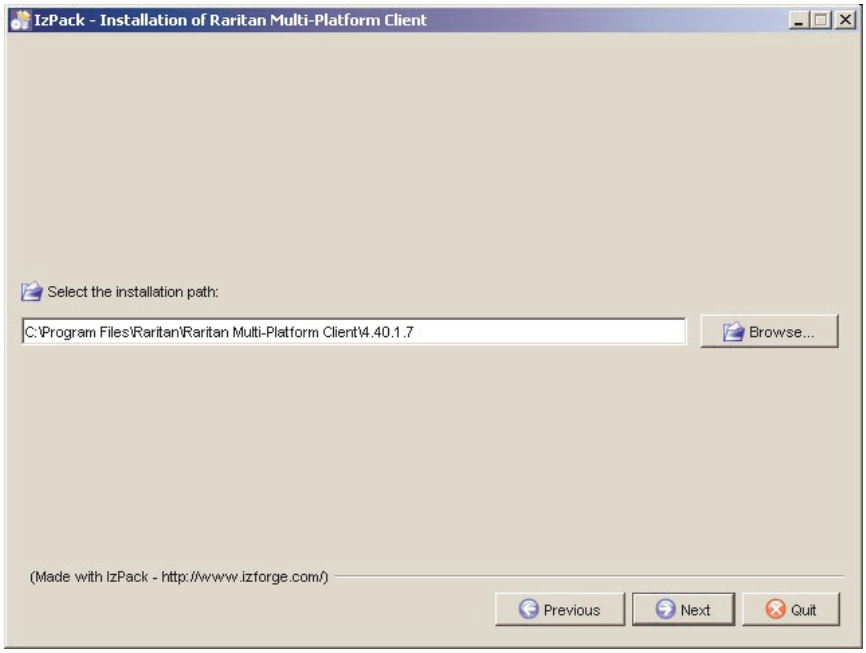
   c. Edit the Path address so that it contains the path to the Java executable.
   For example, if Java is installed on C:\j2re1.4.2_05 and your path is currently set to C:\WINDOWS\SYSTEM32, then change the path to read C:\WINDOWS\SYSTEM32;C:\j2re1.4.2_05

Installing MPC for Windows

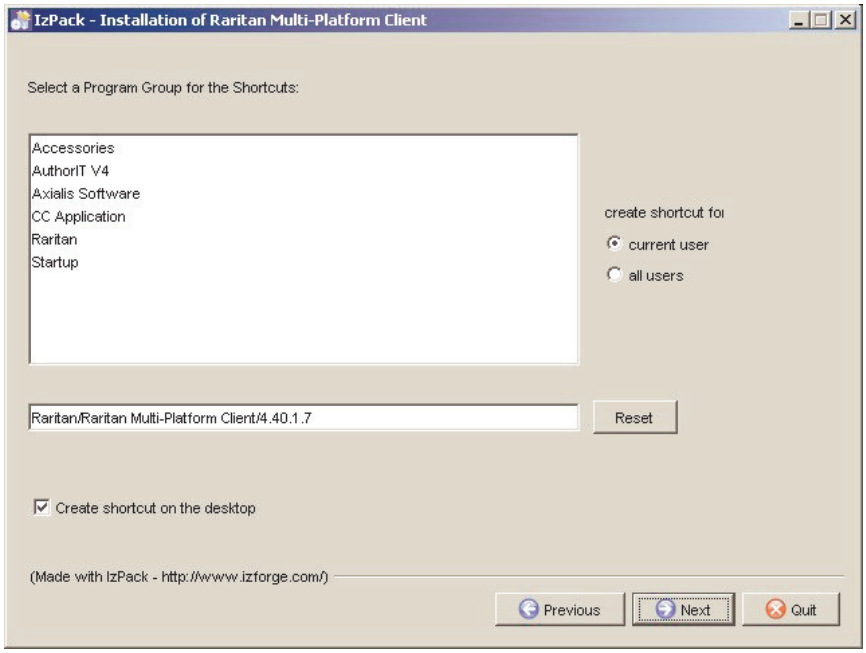
1. Download the MPC-installer.jar installation file or copy the file from a known location. See ***Installing and Launching Standalone MPC*** (see "Installing and Opening Standalone MPC" on page 29) for information on locating the MPC-installer.jar file.

2. Double-click on the jar file icon to open the installation dialog.

3. After the initial dialog appears, click Next.

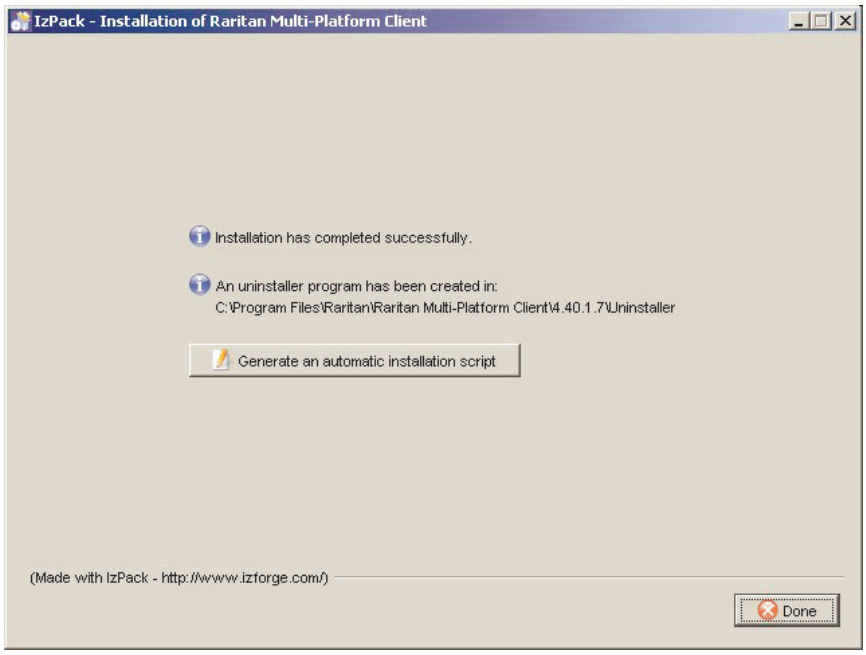


4. Choose the directory where you want to install MPC and click Next. Click Browse to locate a non-default directory.
5. Click Next.



6. In the Shortcut dialog, choose a shortcut location, determine who should have the shortcut, and determine whether you want the shortcut on the desktop. When finished, click Next.

   Once the installation is complete, the final dialog indicates where you will find an uninstaller program and provides an option for generating an automatic installation script. Click Done to close the Installation dialog.



Opening MPC in Windows

1. Click on the Windows Start menu and then choose All Programs > Raritan Multi-Platform Client. Alternatively, double-click the MPC desktop shortcut icon if you created one.
2. Double-click on the desired device in the Navigator to establish a connection.
3. Type your Username and Password in the device dialog and then click OK to log in.

Linux

Java Runtime Environment (JRE) Requirements for MPC

Raritan recommends using Java® Runtime Environment (JRE) version 1.5 for optimum performance but MPC will function with JRE version 1.4.2_05 or greater (with the exception of JRE 1.5.0_02). JRE 1.6 is also supported but has not been fully tested.

Determine your version of the JRE from the Java website: http://www.java.com/en/download/help/testvm.xml.

You may need some configuration depending on your OS and browser. Configuration instructions are provided with the JRE download.

Note: Modem use is not supported with Raritan's Dominion KX101.

Important: When launching MPC from a browser, it is highly recommended that you disable the Java Applet caching.

Although no actual problems have occurred when Java caching is turned on, some non-impacting Java exceptions have occurred. Generation of these Java-exceptions can appear in the Java Applet Console window and may degrade performance.

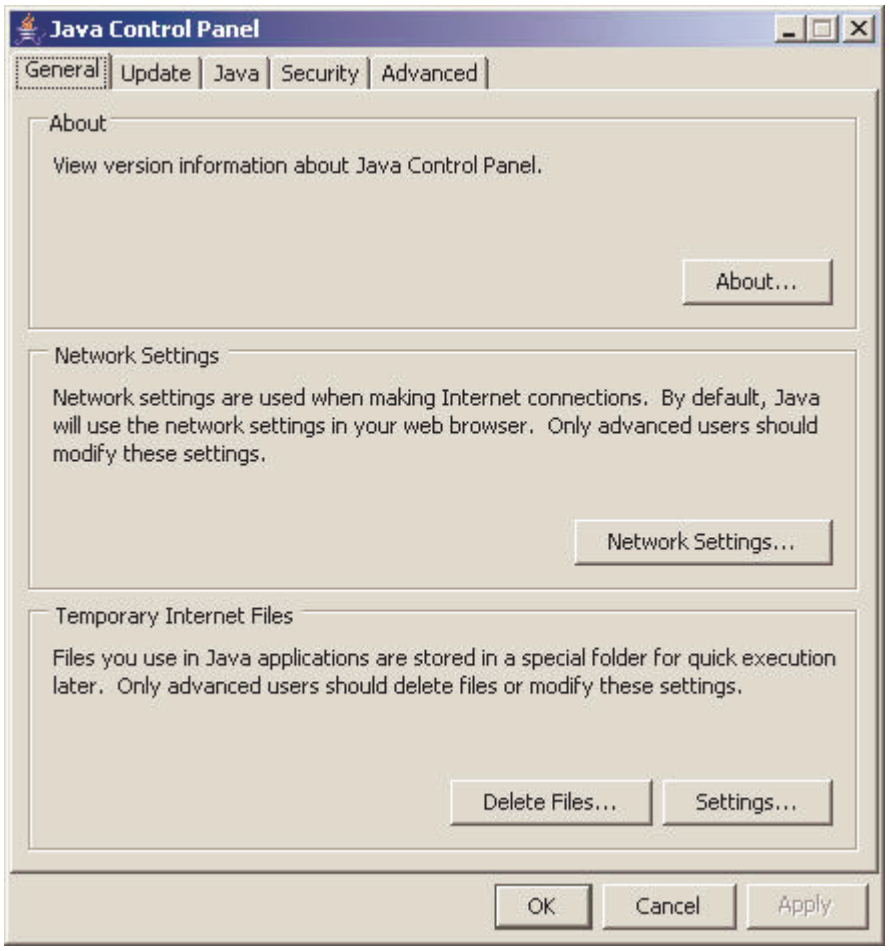
For Linux/UNIX environments, the Java Control Panel is located in the JRE's bin directory; the location varies based on where JRE was installed by your Linux/UNIX administrator.

Tip: It is also recommended that you clear the Java cache.

➢ ***To disable Java caching and clear the cache (use these steps with Microsoft Windows XP and JRE 1.5.0):***

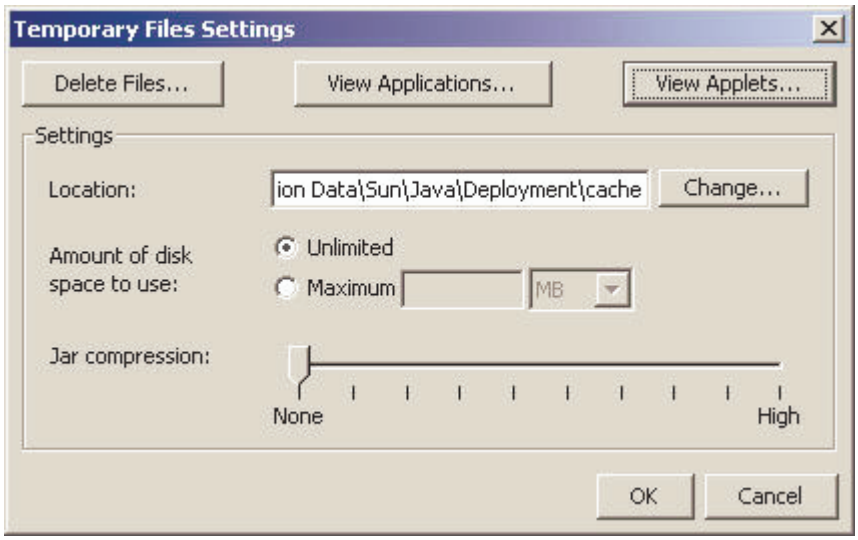
1. From the Start menu, click Control Panel.

2. Double-click on the Java icon to launch it. The Java Control Panel dialog appears.

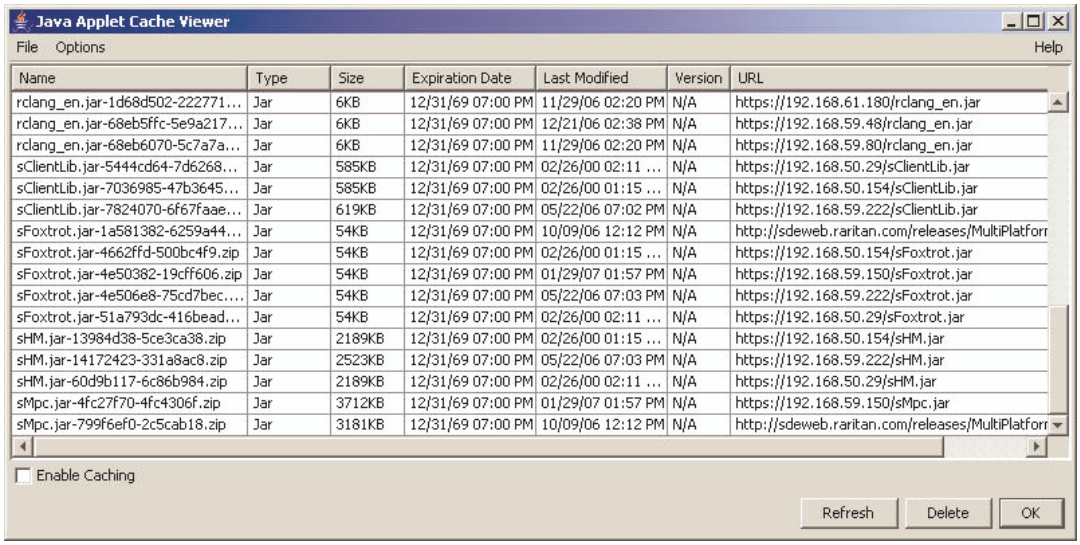


3. To disable Java caching:

a. From the General tab, click the Settings button. The Temporary Files Settings dialog appears.



b. Click the View Applets button. The Java Applet Cache Viewer opens.



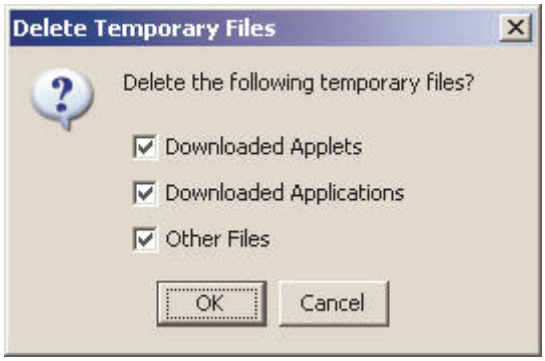
c. Deselect the Enable Caching checkbox if it is already checked.

d. Click OK.

4. To clear the Java cache:

a. From the Temporary Files Settings dialog, click the Delete Files button. The Delete Temporary Files dialog appears.

b. Select the temporary files that you want to delete.



c. Click OK.

Checking JRE Version in Linux

1. In a graphical environment, open a terminal window.
2. Type java version in the command line and press Enter on your keyboard. The currently-installed version of Java Runtime Environment (JRE) is displayed.

   If your path variable is not set to where the java binaries have been installed, you may not be able to see the JRE version.
3. Set your path:

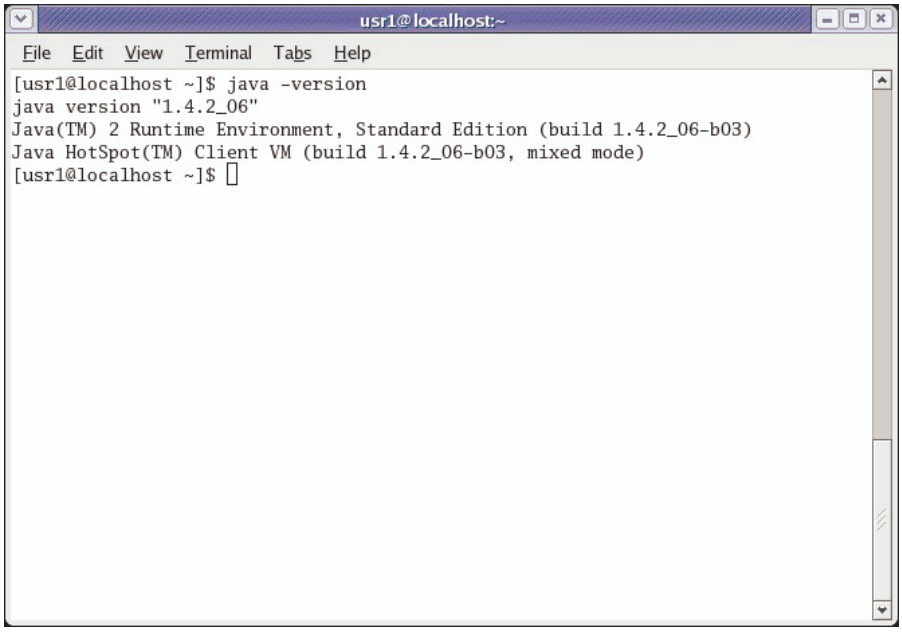
   a. To set your path and assuming JRE 1.4.2_05 is installed in /usr/local/java: you must set your PATH variable.

   b. To set the path for bash shell, export PATH=$PATH:/usr/local/java/j2re1.4.2_05/bin.

   c. To set the path for tcsh or csh, set PATH = ($PATH /usr/local/java/j2re1.4.2_05/bin).

   These commands can be typed at the terminal each time you login. Alternatively, you can add it to your .bashrc for bash shell, .cshrc for csh, or tcsh so that each time you login the PATH is already set.

Refer to your shell documentation if you encounter problems.



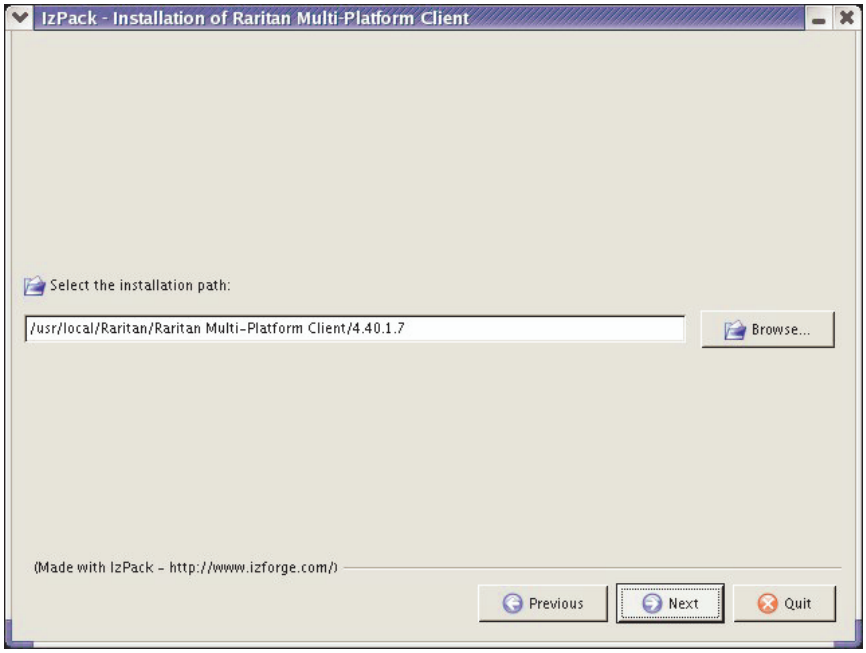
4. If the JRE is version 1.4.2_05 or higher, proceed with the MPC installation. If the version is prior to 1.4.2_05, go to the Java website at http://java.sun.com/products/ to download the latest Runtime Environment.

Installing MPC for Linux

You must have Administrative privileges to install MPC.

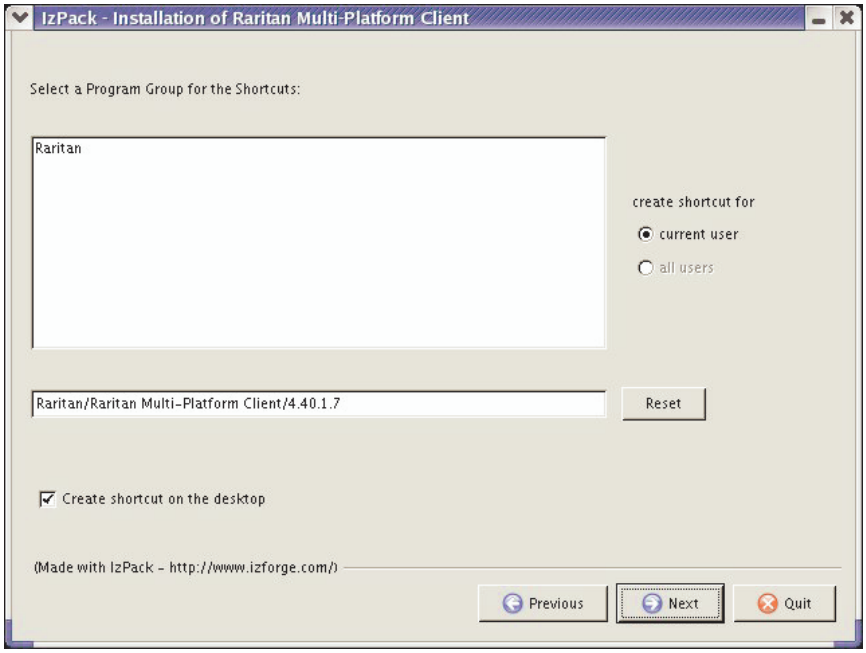
1. Download the MPC-installer.jar file or copy it from a known location.
2. Open a terminal window and open the directory where the installer is saved.
3. Type java -jar MPC-installer.jar and press Enter to run the installer.

4. After the initial page loads, click Next.



5. Use the Browse function to select a directory to install MPC if the directory is different from the default path displayed in the "Select the installation path" field.
6. Click Next to open the Shortcut dialog.
7. On the Shortcut dialog:
   - Choose a shortcut location from the "Select a Program Group for the Shortcuts:" field.
   - Select either "current user" or "all users" to define who should have access to the shortcut.
   - Check the "Create shortcut on the desktop" checkbox if you want the shortcut to appear on the desktop.

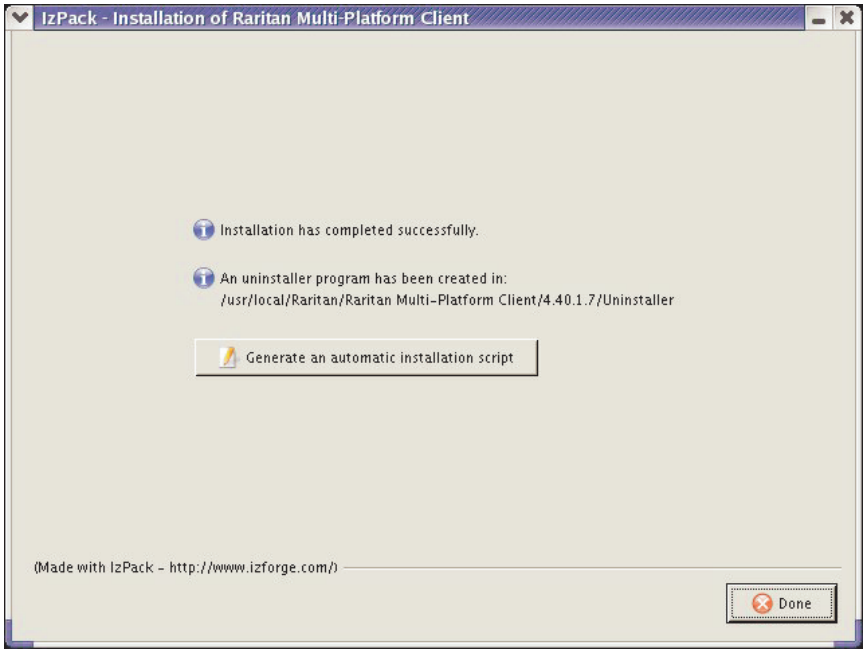
8. When finished, click Next.



Note: Once MPC is installed successfully, a shortcut will be available on the desktop. However, for Linux users, you will need to log out of and then back into your session before the shortcut will be visible on the desktop.

Once the installation is complete, the final page indicates where you will find an uninstaller program and provides you with the option to generate an automatic installation script.

9. Click Done to close the Installation dialog.



Opening MPC in Linux

1. Open a terminal window and change directories to the directory where you installed MPC (default location: /usr/local/Raritan/Raritan MPC/4.40.1.7/).
2. Type ./start.sh and press Enter to open MPC.
3. Double-click on the desired device to establish a connection, type your Username and Password, and click OK to log in.

Solaris

Checking JRE Version on Sun Solaris

1. Launch a terminal window on the Sun Solaris desktop.
2. Type java version in the command line and press Enter. The currently-installed version of Java Runtime Environment (JRE) appears.

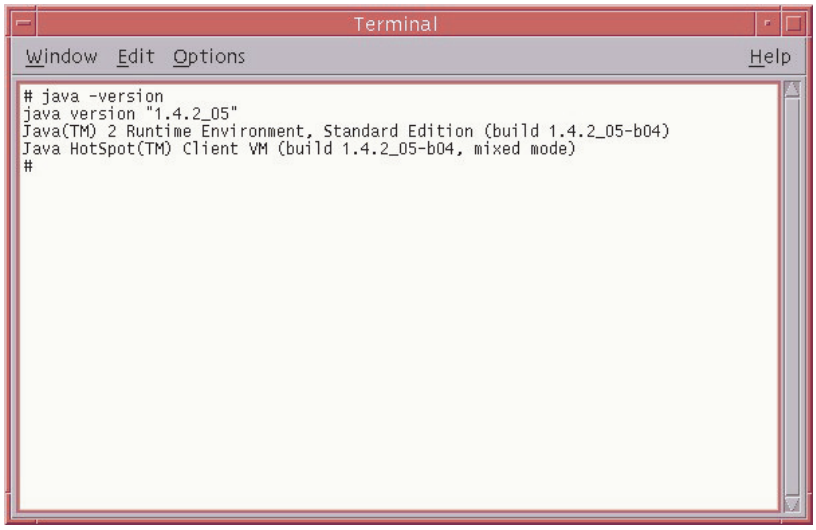
   If your path variable is not set to where the java binaries have been installed, you may not be able to see the JRE version.

   a. To set your path and assuming JRE 1.4.2_05 is installed in /usr/local/java, you must set your PATH variable.

   b. To set path for bash shell, export PATH=$PATH:/usr/local/java/j2re1.4.2_05/bin.

   c. To set path for tcsh or csh, set PATH = ($PATH /usr/local/java/j2re1.4.2_05/bin).

3. These commands can be typed at the terminal each time you login. Alternatively, you can add it to your .bashrc for bash shell, .cshrc for csh, or tcsh so that each time you login the PATH is already set. Refer to your shell documentation if you encounter problems.



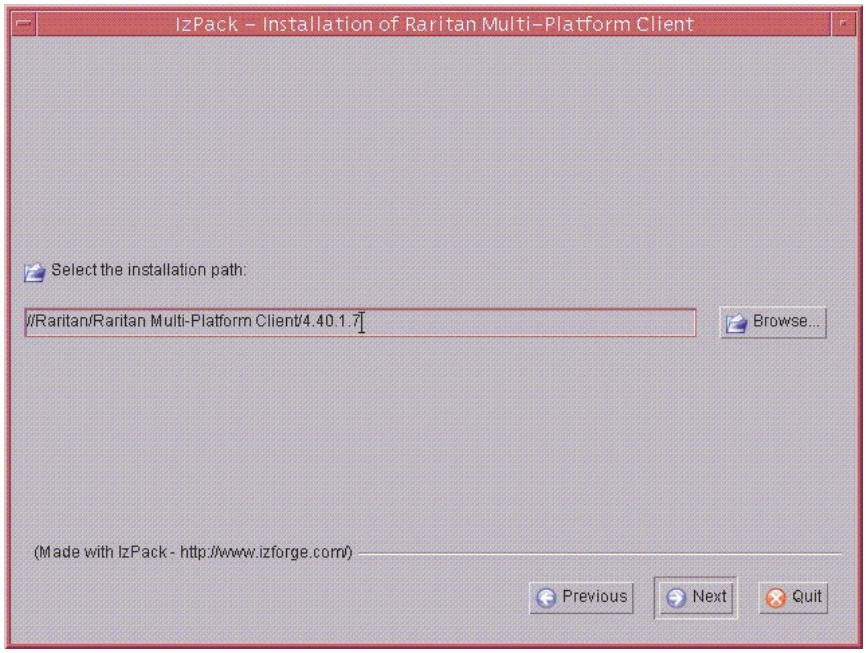
4. If the JRE is version 1.4.2_05 or higher, proceed with the MPC installation. If the version is prior to 1.4.2_05, go to the Sun website at http://java.sun.com/products/ to download the latest Runtime Environment.

Installing MPC for Sun Solaris

You must have administrative privileges to install MPC.

1. Download the MPC-installer.jar file or copy it from a known location.
2. Open a terminal window and navigate to the directory where the installer is saved.
3. Type java -jar MPC-installer.jar and press Enter to run the installer.

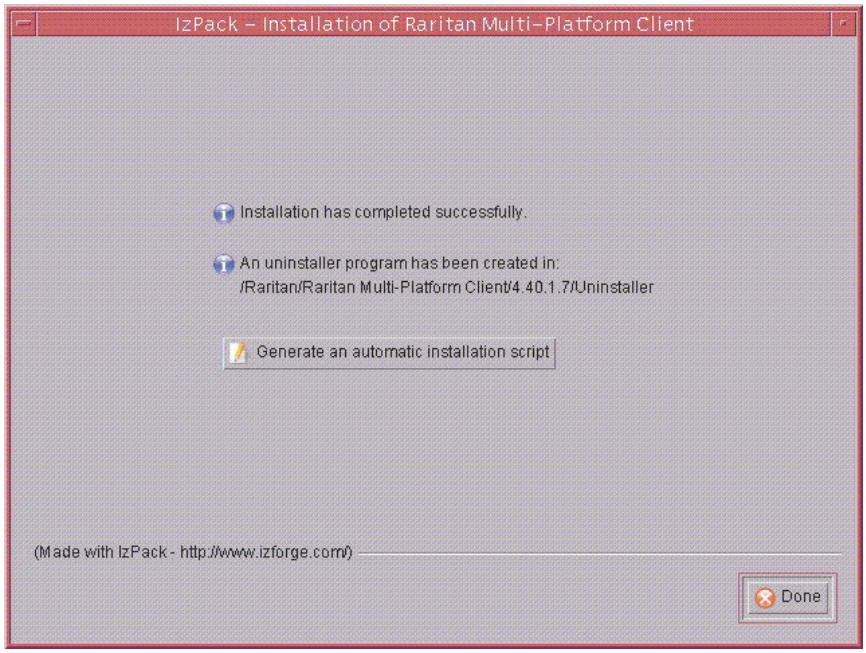
4. After the initial page loads, click Next.



5. Use the Browse function to navigate to the directory you want to install MPC or select the default directory displayed in the "Select the installation path" field.
6. Click Next.
7. When installation is complete, click Next.
8. Click Next again.

   Once the installation is complete, the final dialog will indicate where you will find an uninstaller program and provides the option to generate an automatic installation script.

9. Click Done to close the Installation window.



Opening MPC on Sun Solaris

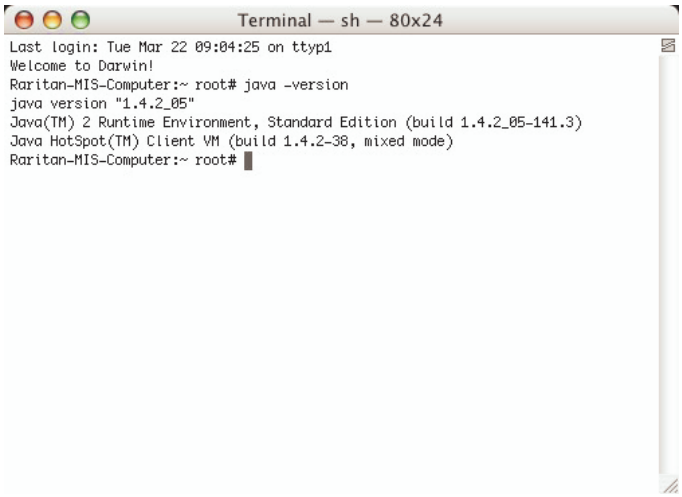
1. Open a terminal window and navigate to the directory where you installed MPC (the default location is /usr/local/Raritan/Raritan MPC/4.40.1.7).
2. Type ./start.sh and press Enter to open MPC.
3. Double-click on the desired device to establish a connection, type your user name and password, and click OK to log in.

Macintosh

Checking JRE Version in Mac OSX

1. Launch a terminal window on the Macintosh desktop.

2. Type the java version in the command line and press Enter. The currently-installed version of the Java Runtime Environment (JRE) is displayed.



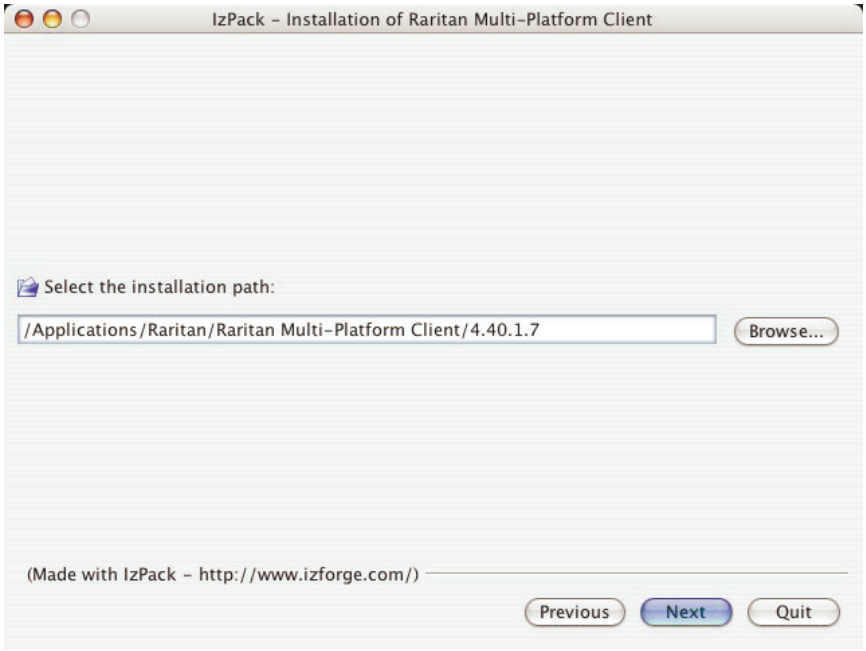
3. If the JRE is version 1.4.2_05 or higher, proceed with the MPC installation. If the version is prior to 1.4.2_05, go to the Apple website to download the latest Runtime Environment.

Installing MPC for Mac OSX

You must have administrative privileges to install MPC.

1. Download the MPC-installer.jar file or copy it from a known location.
2. Open a Finder window and locate the installer.
3. Double click on the MPC-installer.jar file to run the installer.

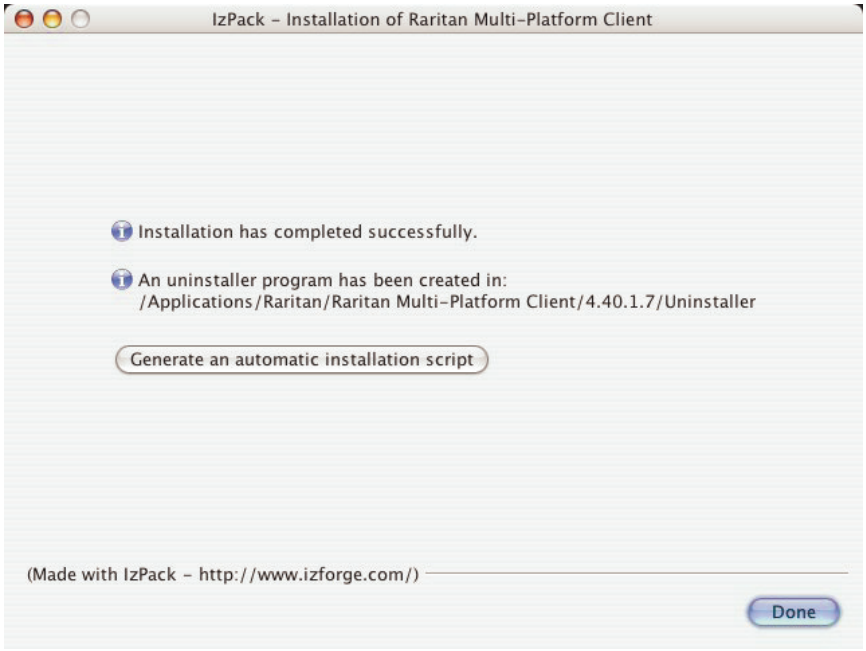
4. After the initial page opens, click Next.



5. Use the Browse function to select a directory to install MPC if the directory is different from the default path displayed in the "Select the installation path" field.
6. When installation is complete, click Next.

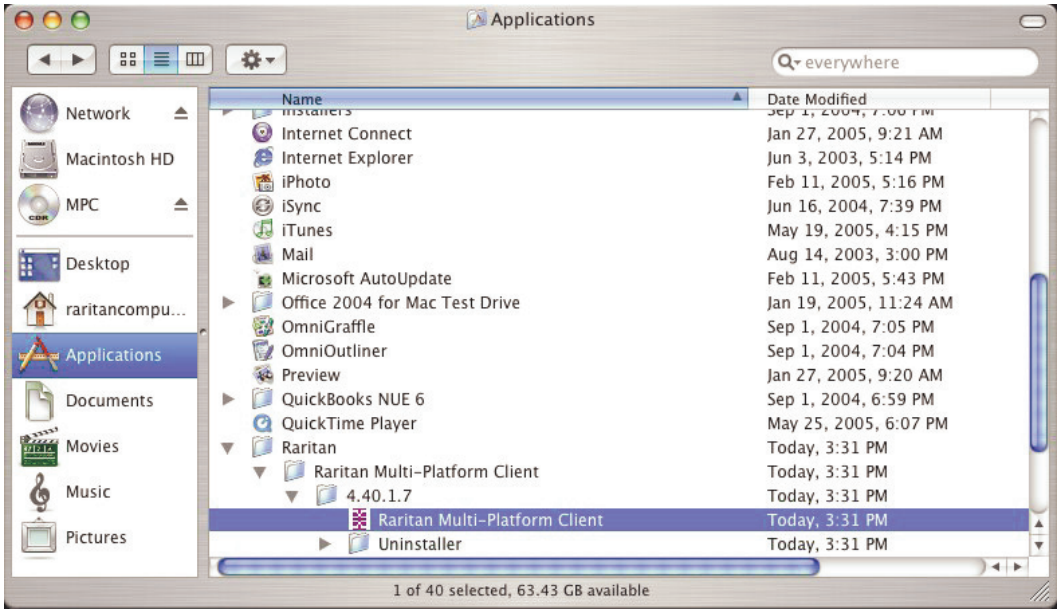
   Once the installation is complete, the final dialog indicates where you will find an uninstaller program and provides you with the option to generate an automatic installation script.

7. Click Done to close the Installation window.



Opening MPC in Mac OSX

1. Open a Finder window and navigate to the directory where you installed MPC (the default location is /Applications/Raritan/Raritan MPC/4.40.1.7).



2. Double-click on the desired device to establish a connection, type your user name and password, and click OK to log in.

RRC Requirements and Installation Instructions

Important: RRC works only with Microsoft Internet Explorer. If you are using a different web browser, MPC will load automatically.

Most users access RRC via Internet Explorer, while other users, particularly those operating over a modem connection, access RRC standalone. Both options are detailed in this guide.

Note: Modem use is not supported with Raritan's Dominion KX101.

RRC Minimum System Requirements

The minimum system requirements for the Raritan Remote Client are:

- CPU Speed: 1.0 GHz
- RAM: 512 Mbytes

Note: Running the client software on system configurations below either of these specifications may impact performance and result in errors.

Opening RRC from a Web Browser

Your IP-Reach and Dominion units feature web browser-access capabilities and can provide a connection from any Windows-based, remote PC running Microsoft Internet Explorer 6.0/7.0.

Security Settings

To access IP-Reach or a Dominion device via the web, your web browser must be configured appropriately on the Internet Explorer security settings tab. Specifically:

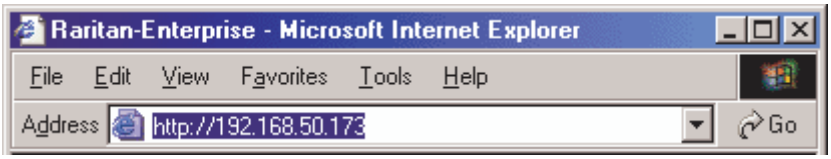
- "Download Signed ActiveX controls" should be set to either Enable or Prompt.
- "Run ActiveX controls and plug-ins" should be set to either Enable or Prompt.

Consult your Microsoft Internet Explorer documentation for additional information.

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 settings in Internet Explorer. Consult your Microsoft Windows documentation for more information.

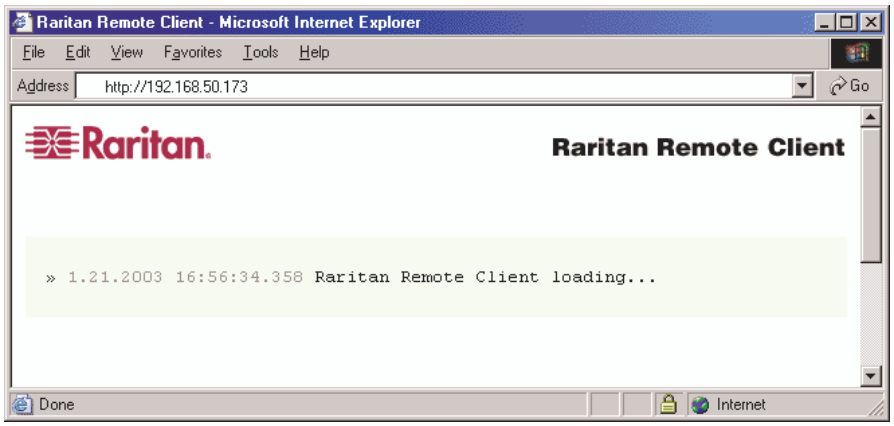
Opening RRC

1. Ensure that your browser security settings are configured appropriately and type the IP address assigned to your IP-Reach or Dominion unit in the URL field of your web browser. See the Initial Configuration section in the device user guide for additional information on configuring IP addresses.

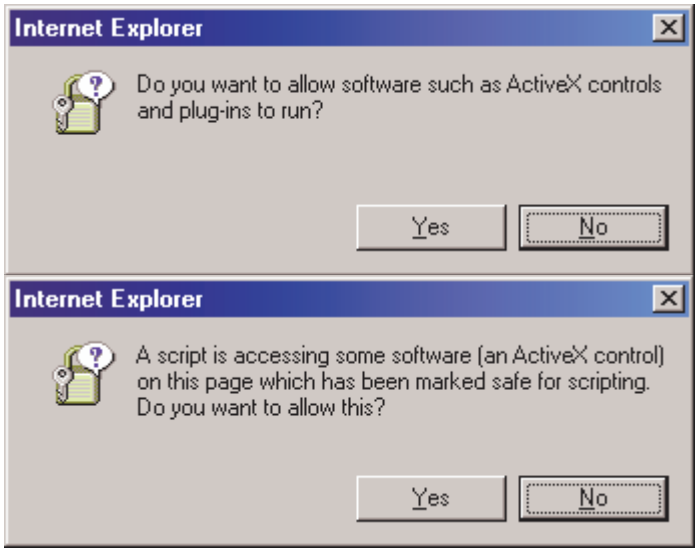


Note: IP-Reach and Dominion units ship with the default IP address of 192.168.0.192. Note that an IP address must be used. Host names are not currently supported.

You will be redirected to an HTTPS (128-bit) secure webpage so you can open RRC.



2. Depending on your browser and its security configuration, you may see any or all of the following dialogs asking you to confirm you want to access and open an externally-provided application. Click Yes to accept these prompts.



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.

➢ ***To remove cached files in Internet Explorer v6.0:***

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

Installing and Opening Standalone RRC

Note: This step is optional. IP-Reach or Dominion can be accessed from a remote PC either by installing RRC software or by opening RRC via a web browser. Accessing IP-Reach or Dominion via a web browser does not require any software installation on a remote PC.

This section lists the steps required to invoke RRC using standalone software, which may be useful for accessing IP-Reach or Dominion 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 website (http://www.raritan.com/).
2. Click Support in the top navigation bar and then click Firmware Upgrades in the left navigation panel (or type the URL http://www.raritan.com/support/firmwareupgrades).
3. Scroll down the page until you see the appropriate product name and click on it.
4. Locate the version of the standalone RRC client you are using. 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. Download the .zip file or simply click on the .zip file entry.
6. Double-click on the installer executable in the .zip file and follow the instructions in the InstallShield Wizard to complete the RRC installation. Be sure to check the release notes for the latest information and any release specific instructions.

   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 they are installed, you will be asked to restart your PC after the installation.
7. A Raritan Remote Client icon will appear on your desktop after the installation is complete. Click on this icon to open the standalone RRC application.

   The standalone application can be uninstalled using the Add or Remove Programs function in the Windows Control Panel.

Note: You must uninstall the application before installing a new version of standalone RRC.

Modem Connectivity in MPC

➢ ***To make modem connectivity available on Unix, Linux, and Mac OS for non-root users:***

1. As the root, change the group for /etc/ppp directory and required files:
   a. chgrp uucp /etc/ppp
   b. chgrp uucp /etc/ppp/pap-secrets
   c. chgrp uucp /etc/ppp/peers
2. Change the permissions for /etc/ppp chmod g+rwx /etc/ppp
3. Change the permissions for /etc/ppp/pap-secrets chmod g+rwx /etc/ppp/pap-secrets
4. Change the permissions for /etc/ppp/peers chmod g+rwx /etc/ppp/peers
5. Set the suid bit to pppd chmod u+s /usr/sbin/pppd (/usr/bin/pppd depending on the location of pppd)
6. Assign users to the uucp group:
   a. /usr/sbin/usermod -G {existing groups for user1},uucp user1
   b. /usr/sbin/usermod -G {existing groups for user2},uucp user2, etc.
7. When logged in as the normal user, update the path for access to pppd and the chat export PATH=$PATH:/usr/sbin (/usr/bin depending on the location of pppd).

Note: For both root and non-root users, ensure that the options file exists under /etc/ppp

Operation

Note: Unless otherwise indicated, the contents of this section are the same in MPC and RRC.

Connection Profiles

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

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

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

Connection profiles are created, modified, deleted, established, and closed in the same way for both MPC and RRC.

Creating Profiles

➢ ***To create a profile:***

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

   The Add Connection dialog appears. Options are organized into three tabs.
2. On the Connect tab, type a meaningful description of the device in the Description field (up to 32 alphanumeric, ***special characters*** (see "Special Characters in MPC" on page 144) characters are allowed). This description identifies the Raritan device in the Navigator.
3. From the Product drop-down, choose the Raritan product you are using.
4. Select the Connection Type from the drop-down to specify the type of connection.

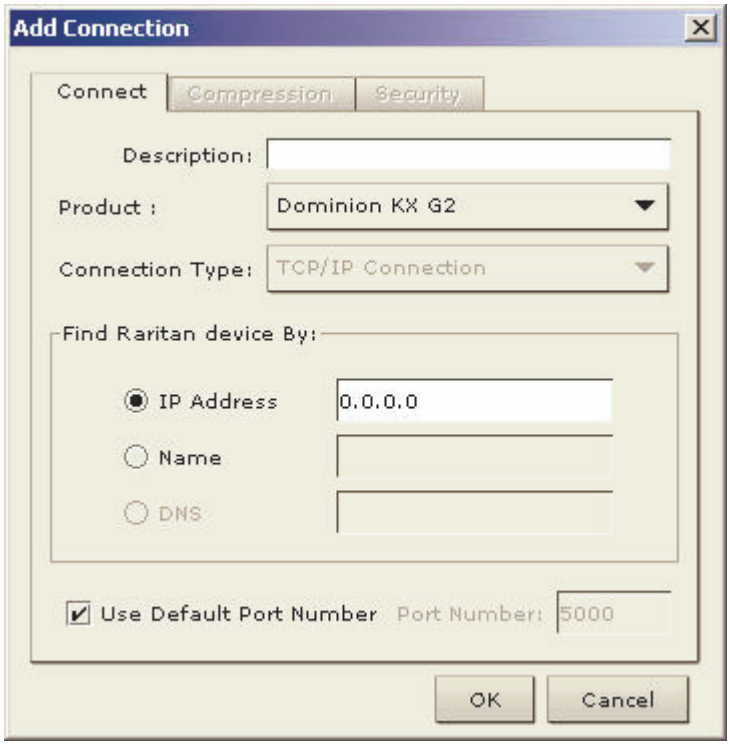
   Note: Only TCP/IP is available for Generation 2 (G2) Raritan devices.

   ---

   a. If TCP/IP Connection is selected for a LAN/WAN connection, complete the information in the Find Raritan device By section:
   - Type the IP Address assigned to your Raritan device.

- Type the name assigned to your Raritan device during initial setup.
- Type the Domain Name Server (DNS) name. Use this option if you use a DNS server to resolve a DNS name to the IP Address assigned to your Raritan device.

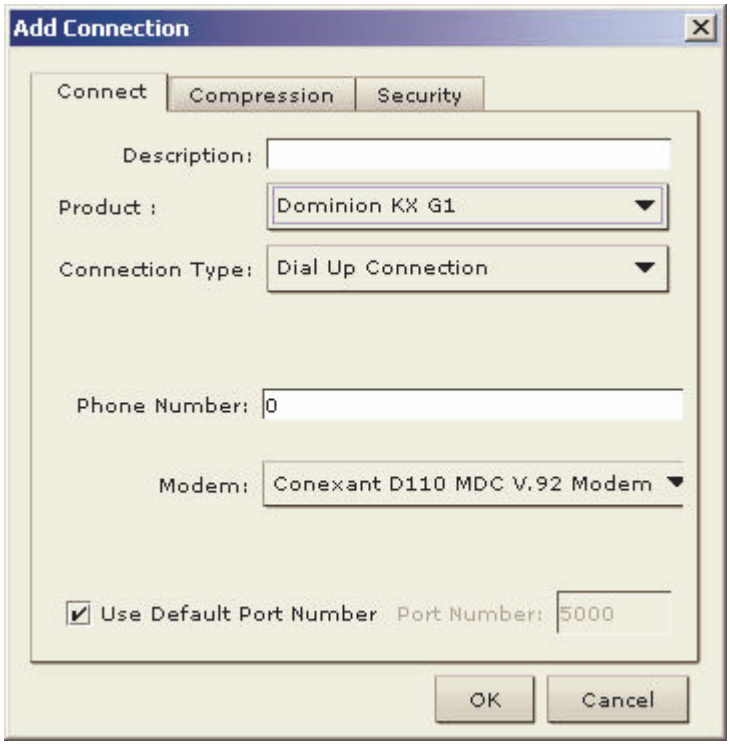
Note: You cannot use this option for Raritan Generation 2 (G2) devices.



a. Select Dial Up Connection from the Connection Type drop-down for a direct analog modem connection to the Raritan device. Type the parameters that MPC or RRC should use to establish a connection. Dial up connection does not apply to Generation 2 (G2) or KX101.

- Enter the phone number for the dial-up connection. Remember to include any additional codes that should be dialed to establish a connection, such as country codes, area codes, or outside line access codes.
- Select the modem (as configured in Windows) from the drop-down list that will be used to dial and connect to your Raritan device.

Note: For security reasons, you must use the MPC standalone client if you require modem access. Further, one modem on a client PC can be used for only one device connection.



- Check Use Default Port Number to use the default port number (5000). For TCP Ports, Dominion KX and IP-Reach are automatically configured to use TCP Port 5000 when communicating with MPC/RRC. If you do not want to use the default port number, uncheck the checkbox and type the port number in the Port Number field.

1. Update the Compression tab (not available for Generation 2 (G2) Raritan devices):

   a. Select the Connection Speed from the drop-down. IP Reach and Dominion can automatically detect available bandwidth and not limit bandwidth use, but you can also adjust this usage according to bandwidth limitations. Depending on the Raritan device in use, different options may be available.

- Auto Detect
- 100mb Ethernet
- 10mb Ethernet
- 1.5mb (Max DSL/T1)
- 1mb (Fast DSL/T1)
- 512 kb (Medium DSL/T1)
- 384 kb (Slow DSL/T1)
- 256 kb (Cable)
- 128 kb (Dual ISDN)
- 56 kb (ISP Modem)
- 33 kb (Fast Modem)
- 24 kb (Slow Modem)

a. Select the Color Depth from the drop-down. IP-Reach and Dominion can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidth constraints. Depending on the Raritan device in use, different options may be available.

- Auto Select Color
- 15-bit RGB Color
- 12-bit RGB Color
- 8-bit RGB Color
- 5-bit Color
- 4-bit Color
- 4-bit Gray
- 3-bit Gray
- 2-bit Gray
- Black and White

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

---

a. Select Progressive Update to increase the usability in constrained bandwidth environments. When Progressive Update is enabled, IP-Reach or Dominion initially sends an image of the remote desktop at lower color depths, and then provides higher color depth images as bandwidth allows.

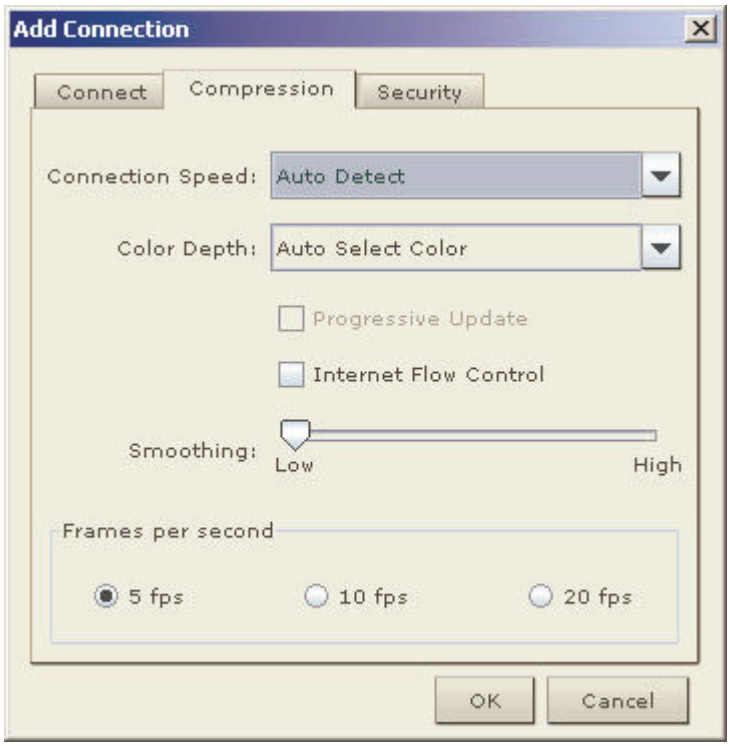
Note: When Color Depth is set to Auto Select Color (default), Progressive Update is automatic. IP-Reach or Dominion will enable/disable Progressive Update as required, disabling it for fast connections and enabling it for slow connections.

b. When using IP-Reach or Dominion over an unpredictable public WAN (particularly in international scenarios), checking the Internet Flow Control checkbox ensures that packets transmitted by IP-Reach or Dominion are received and reconstructed by MPC/RRC in the correct order.

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

d. Select "Frames per second". This setting instructs MPC on how often to redraw the video display of the target. This only affects the client display behavior and has no bearing on the data rate of the video being sent to the client. Setting this option higher makes the video appear smoother but also requires more processing power.

Note: "Frames per second" option is only available in MPC.



1. Update the Security tab.

   Note that the Security tab is disabled for Generation 2 Raritan devices. If your Dominion or IP-Reach unit is configured to use a private security key, input that key to gain the authorization required to initiate a connection to that IP-Reach or Dominion unit.

   a. Type the private security key in the Private Key field.

   b. Retype the private security key in the Confirm Private Key field to ensure no typographical errors were made.

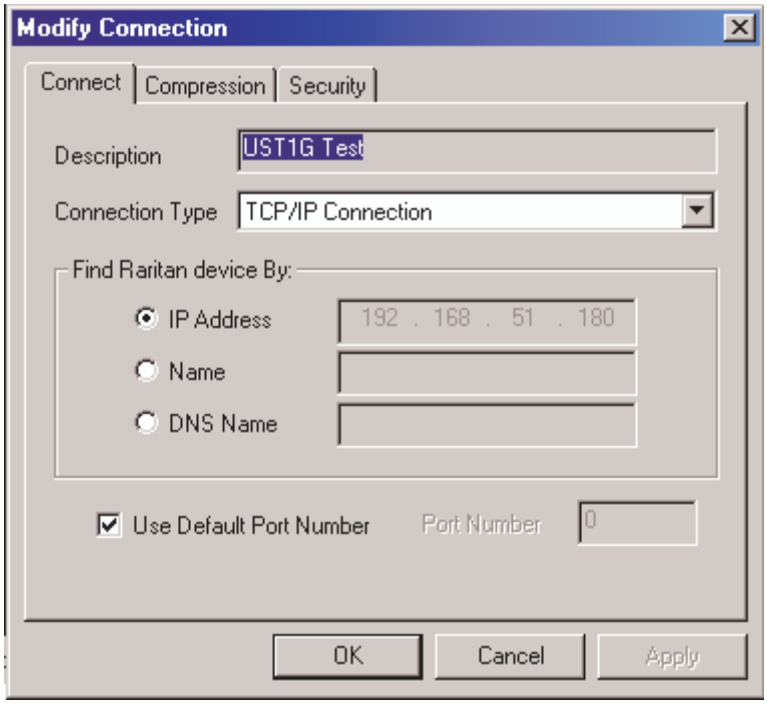
2. Click OK to create the connection profile.

Modifying Profiles

➢ ***To modify a profile in MPC or RRC:***

1. Select the device in the Navigator panel and right-click on it.

2. Choose Modify Profile. The Modify Connection dialog appears.



3. Update the fields as appropriate.
4. Click OK.

Deleting Profiles

➢ ***To delete a profile in MPC or RRC:***

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

Establishing a New Connection

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

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

Note: The default IP-Reach or Dominion login user name is admin and the default password is raritan. You have administrative privileges using these login credentials.

Passwords are case sensitive and must be entered in the exact case combination in which they were created. To ensure security, change the default user name password as soon as possible.

If you do not see an icon for your IP-Reach or Dominion device in the Navigator, follow the instructions in the ***Creating Profiles section*** (see "Creating Profiles" on page 53) to create a new connection profile.

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

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

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

Closing a Remote Connection

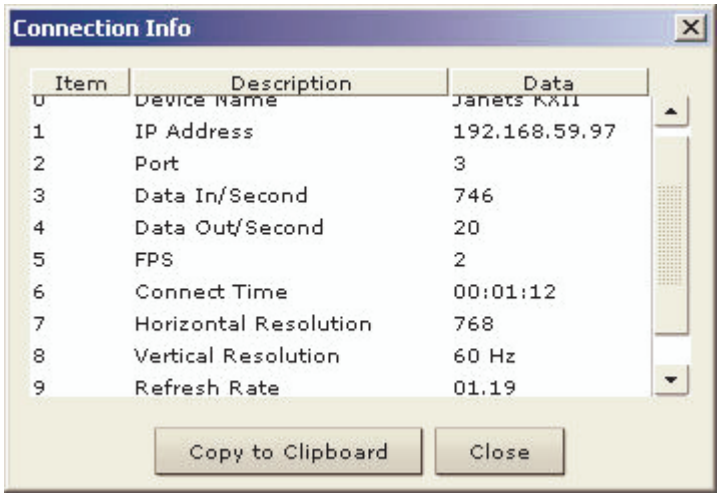
1. To close the IP-Reach or Dominion connection, select the device in the Navigator and right-click on it.
2. Choose Disconnect from the shortcut menu.
3. To exit MPC or RRC completely, click Exit on the Connection menu.

MPC Connection Information

Note: RRC can support only one modem connection at one time.

➢ ***To obtain information about your MPC connection:***

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



The following information is displayed about the current connection:

Connection information	Description
Device Name	The name of your Dominion or IP-Reach device.
IP Address	The IP Address of your Dominion or IP-Reach device.
Port	The KVM Communication TCP/IP Port used to access the target device.
Data In/Second	Data rate in.
Data Out/Second	Data rate out.

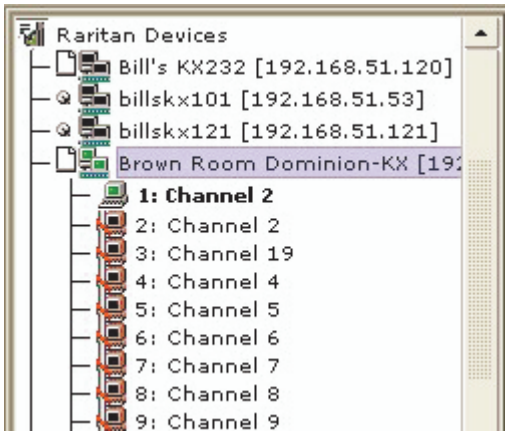
Connection information	Description
FPS	The frames per second transmitted for video.
Connect Time	The duration of the connect time.
Horizontal Resolution	The page resolution horizontally.
Vertical Resolution	The page resolution vertically.
Refresh Rate	How often the page is refreshed.
Protocol Version	The RFB Protocol version.

➢ ***To copy this information:***

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

Connect to a Remote KVM Console

Once you establish a connection with a Raritan IP-Reach or Dominion device, that unit's icon in the navigator expands to display all ports enabled for remote access.



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

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

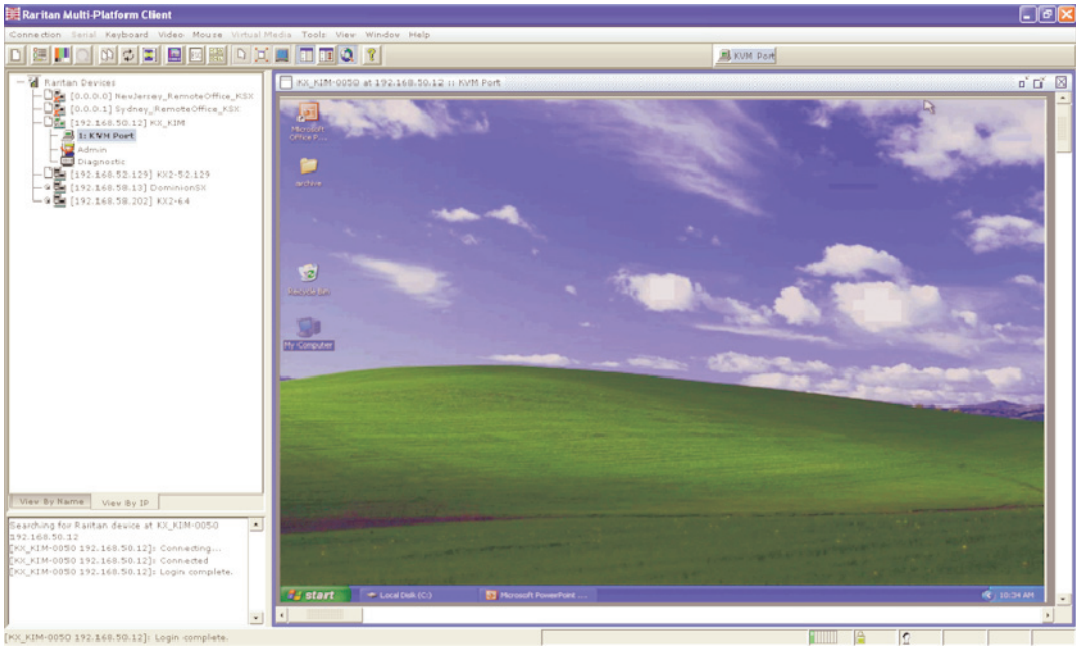
Once connected, Raritan KVM over IP devices display real-time video output of the target server (this video is compressed and encrypted according to the configuration settings specified by the administrator). You now have complete, low-level control of the KVM console as if you were physically located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

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

Window Layout

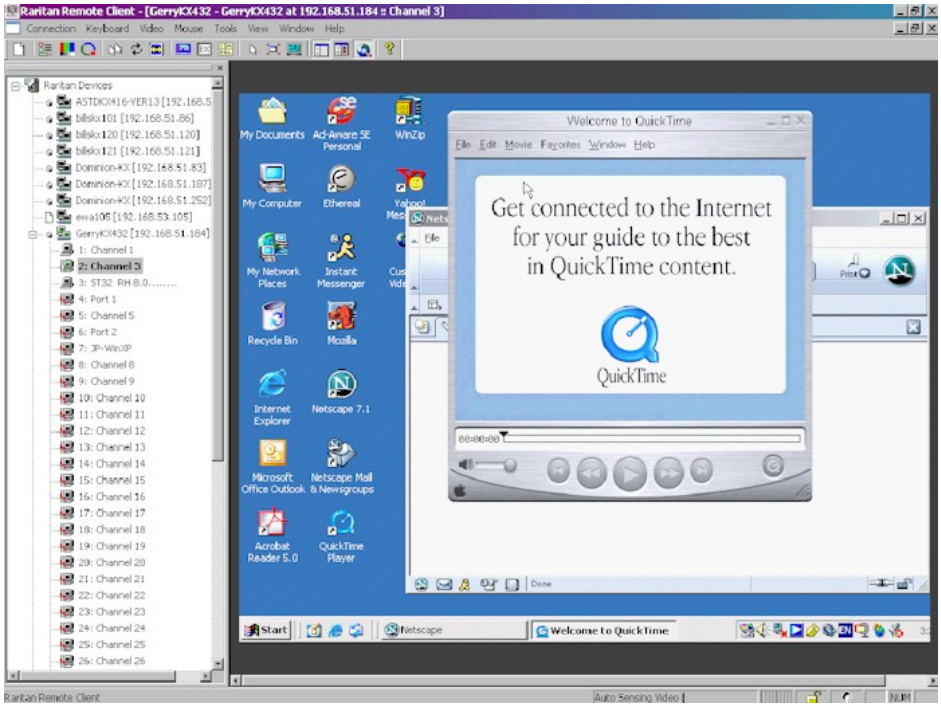
MPC Interface

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



RRC Interface

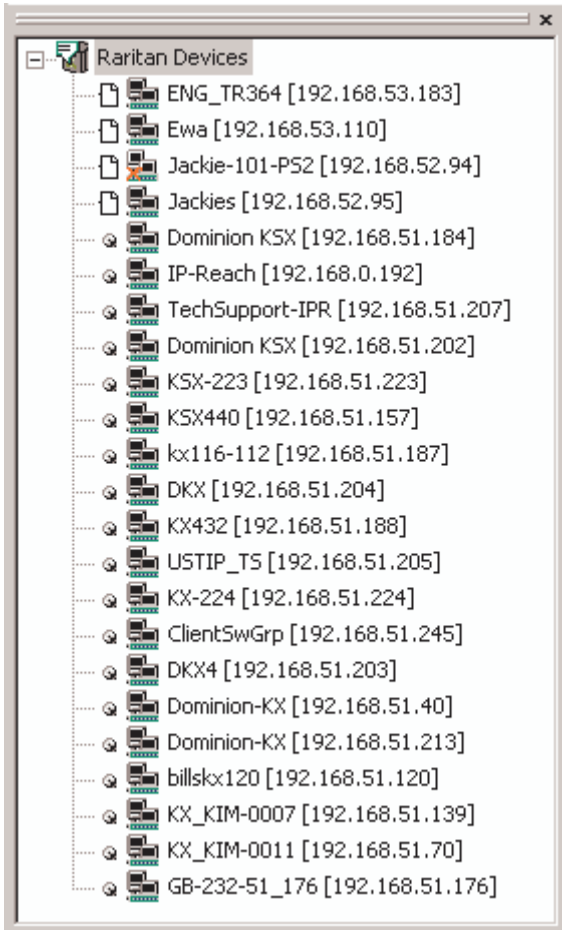
The RRC window is almost identical to the MPC window.



Navigator

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

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



Devices

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

In RRC, profiled devices are listed in the Navigator according to the data in the Description field of the device's profile. Automatically-identified devices will be identified according to the name assigned to them in that device's network configuration setting.

Device Ports

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

If no name is assigned to a port, by default it is listed as 'Unnamed' in the Navigator. So, if you create a port and do not provide a name for it or if you delete an existing port's name, it will be use 'Unnamed' when you reconnect to the device.

If all device ports to which you are connecting are already occupied, an alert message appears and you must wait until one of the ports is available in order to connect.

Navigator Icons

Each device in the Navigator is assigned two icons. One icon represents the device's connection profile and the other icon represents its network status. A connection profile is generally created by a user in order to store personalized information about specific devices (see *Creating Profiles* (on page 53) for additional information). The connection status indicates the current status of the device.

Device Connection Profile Icons (Left Icon)

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

Device Network Status Icons (Right Icon)

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

Port Connection Status Icons

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

Icon	Description
	Connected
	Available for connection.
	Unavailable (either no device is connected or access is blocked).

Icon	Description
	In use by another user (may be unavailable depending on permissions).

Customizing the Navigator

Navigator Customization

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

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

MPC Navigator Tabs

MPC tabs at the base of its Navigator pane. These tabs allow you to change how you display devices.

Click the View By Name tab to sort the list alphabetically by name or click the View By IP tab to sort the list numerically by IP address.

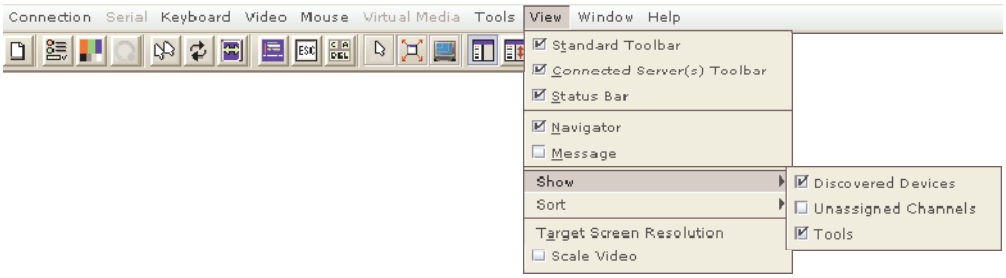
Note that these tabs are available only in the MPC interface.

Display and Sorting Options

To better organize your view of all ports, use the Show and Sort options in the View menu. Note that you do not need an open connection to a target to show and sort targets in the Navigation panel.

Showing Ports

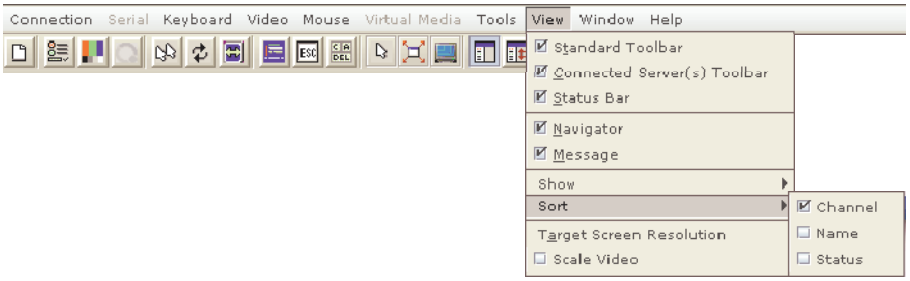
- Discovered Devices: Shows or hides discovered devices from the Navigator view. You will not see broadcast messages when this option is disabled (not selected).
- Unassigned Channels: Shows or hides channels with no assigned targets. Note that the default for Generation 1 (G1) devices is to show unassigned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



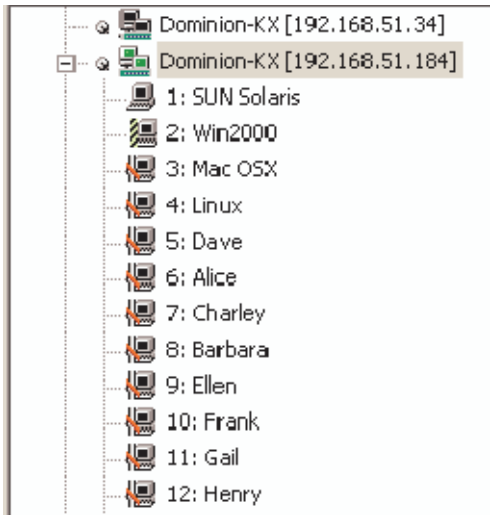
Note: These settings are saved from session to session.

Sorting Ports

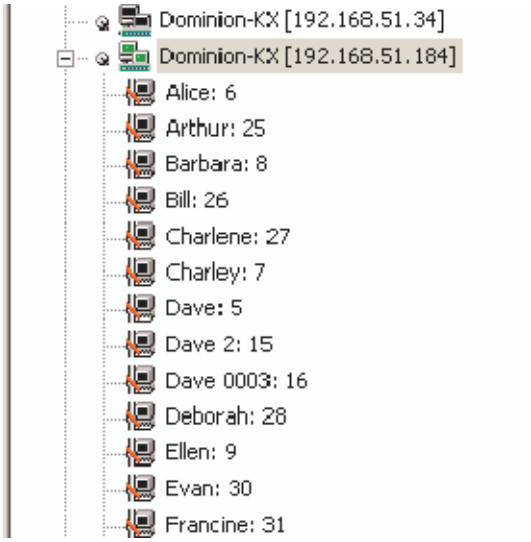
Use the Sort options on the View menu to organize port information. You are able to sort ports by channel number, channel name, or channel status.



Channel Number: When sorted by channel (View > Sort > Channel), ports are listed numerically.

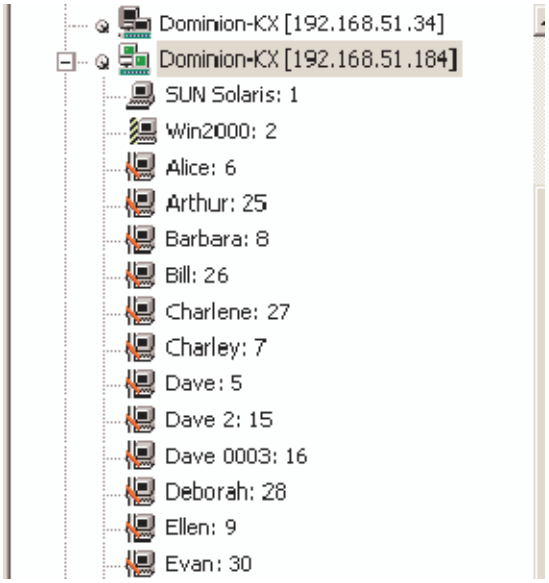


Name: When sorted by name (View > Sort > Name), port names are sorted alphanumerically within each group.



Status: When sorted by status (View > Sort > Status), ports are sorted in the following order:

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



Toolbars

Standard Toolbar

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

➢ ***To display the Standard toolbar:***

- Choose View > Standard Toolbar.

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

Button	Button Name	Description
	New Profile	Creates a new Navigator entry for a Raritan device. Same result as choosing Connection > New Profile in the menu.
	Connection Properties	Opens the Modify Connection Properties dialog from which you can manually adjust bandwidth options (such as connection speed, color depth, and so forth). Same as choosing Connection > Properties or choosing Connection Properties on the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.
	Video Settings	Opens the Video Settings dialog, allowing you to manually adjust video conversion parameters. Same as choosing Video > Video Settings or choosing Video Settings on the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.
	Color Calibration	Adjusts color settings to reduce excess color noise. Same as choosing Video > Color Calibrate.

Button	Button Name	Description
	Synchronize Mouse	In dual-mouse mode, forces realignment of the target server mouse pointer with the mouse pointer. Same as choosing Mouse > Synchronize Mouse or choosing Synchronize Mouse on the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.
	Refresh Screen	Forces a refresh of the video screen. Same as choosing Video > Refresh Screen or choosing Refresh Screen on the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.
	Auto-sense Video Settings	Forces a refresh of the video settings (resolution, refresh rate). Same as choosing Video > Auto-sense Video Settings.
	Enter On-Screen Menu	Not applicable for IP-Reach or Dominion. Used by the application with other Raritan products. Same as choosing Keyboard > Enter On-Screen Menu.
	Exit On-Screen Menu	Not applicable for IP-Reach or Dominion. Used by the application with other Raritan products. Alternatively, select Esc on the keyboard. Same as choosing Keyboard > Exit On-Screen Menu.
	Send Ctrl+Alt+Del	Sends a Ctrl+Alt+Del hot key combination to the target server. Same as choosing Keyboard > Send Ctrl+Alt+Del.

Button	Button Name	Description
	Single Cursor Mode	Starts Single Cursor mode in which the local mouse pointer no longer appears onscreen. Same as choosing Mouse > Single Cursor Mode. Press Ctrl+Alt+X to exit this mode. Alternatively, choose Single/Double Cursor from the shortcut menu, which is opened by pressing Ctrl+Left Alt+M.
	Full Screen Mode	Maximizes the screen real estate to view the target server desktop. Same as choosing View > Target Screen Resolution (in MPC) or Full Screen (in RRC). Alternatively, press Ctrl+Left Alt+M to open the shortcut menu and then choose Full/Normal Screen or press the F key on your keyboard.
	Scaling	Increases or reduces the target video size so you can view the entire contents of the target server window without using the scroll bar.
	Show/Hide Navigator	Toggles the Navigator panel between visible and hidden. Same as choosing View > Navigator.
	Refresh Navigator	Forces a refresh of the data displayed in the Navigator.
	Show/Hide Browse All Devices	Toggles between displaying and not displaying Raritan devices in the Navigator that are automatically identified on the network and that do not have preconfigured profiles associated with them.
	About	Displays the application version information. Same as choosing Help in the menu bar.

Connected Server(s) Toolbar

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

Note: The Connected Server(s) Toolbar does not appear in Single Mouse mode.

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

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

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

- Choose View > Connected Server(s) Toolbar.

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

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

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

Status Bar

The status bar displays session information about your connection to a Raritan IP-Reach or Dominion device. This information includes:

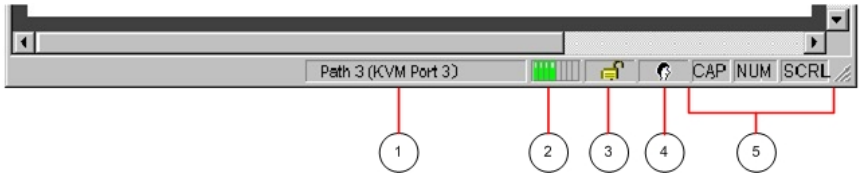


Diagram key	Session information	Description
1	Video sensing status/path indicator	Indicates when video sensing occurs during connections to target KVM server ports.
2	Bandwidth usage indicator	Indicates how much of your total available bandwidth is currently being used. The connection speed setting determines total available bandwidth. This setting is defined on the Compression tab of the Connection Properties dialog, which is accessed by choosing Connection > Properties, or pressing Ctrl+Left Alt+ M and then choosing Connection Properties.
3	Security indicator	Indicates whether the current remote connection is protected by encryption. Encryption requirements are set during IP-Reach or Dominion configuration of your Raritan KVM over IP device. When a Raritan IP-Reach or Dominion device is configured for no encryption or SSL authentication, the Security Indicator is represented on the status bar by an open lock icon. When SSL authentication, data encryption, or SSL encryption is applied, the security indicator is represented on the status bar by a closed lock.

Diagram key	Session information	Description
4	Concurrent connections indicator	Indicates that multiple remote users are currently connected to the same IP-Reach or Dominion target server on the device. One icon indicates a single user is connected and two icons indicates two or more users are connected. Concurrent connection ability can be set globally under PC share mode on the Manager Security Settings page or set per individual user in the Concurrent Access Mode setting on the KX Manager User Account Settings page. For Dominion KX II, concurrent connection ability can be set using the PC Share Mode option in the Dominion KX II Security Settings page: PC-Share permits concurrent access and Private limits server access to one user at a time.
5	Lock key indicators	Indicates the status of the current target KVM Server, in respect to the activation of the Caps-Lock, Num-Lock, and Scroll-Lock keys. If these keys are enabled on the target server being viewed, this affirmative status will be reflected on the status bar.

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

Screen Modes

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

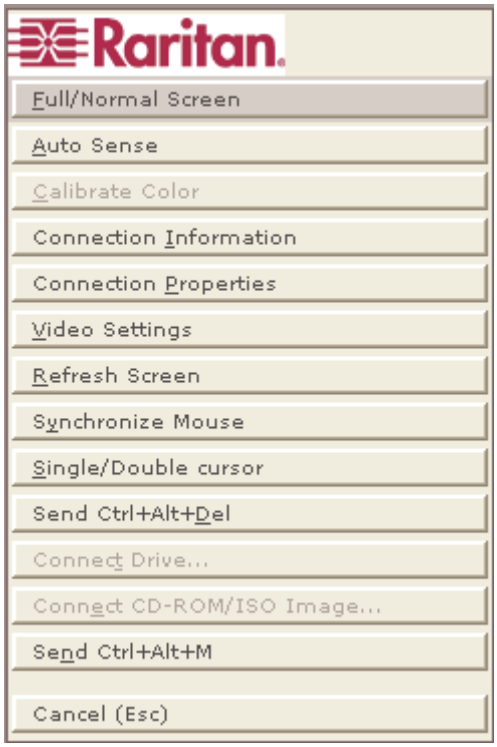
This option it is called Full Screen mode in RRC and Target Screen Resolution mode in RRC. In both applications, you can click the Full Screen button  on the toolbar to activate Full Screen mode or use the Ctrl+Left Alt+M+F hot key combination to enable it.

MPC Target Screen Resolution Mode

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

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

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

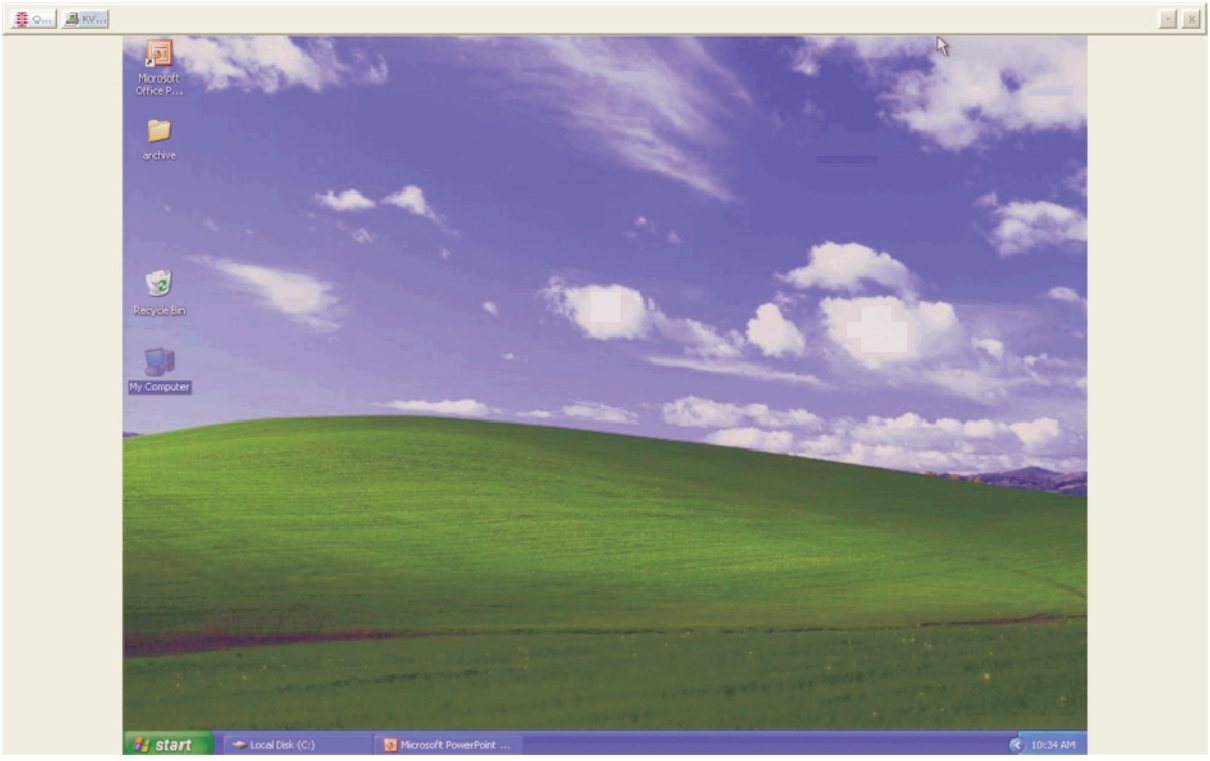


To exit full screen mode, use the shortcut menu or click the Close icon  that appears at the top right of the page when you hover your mouse along the top of the screen.

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

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

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



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

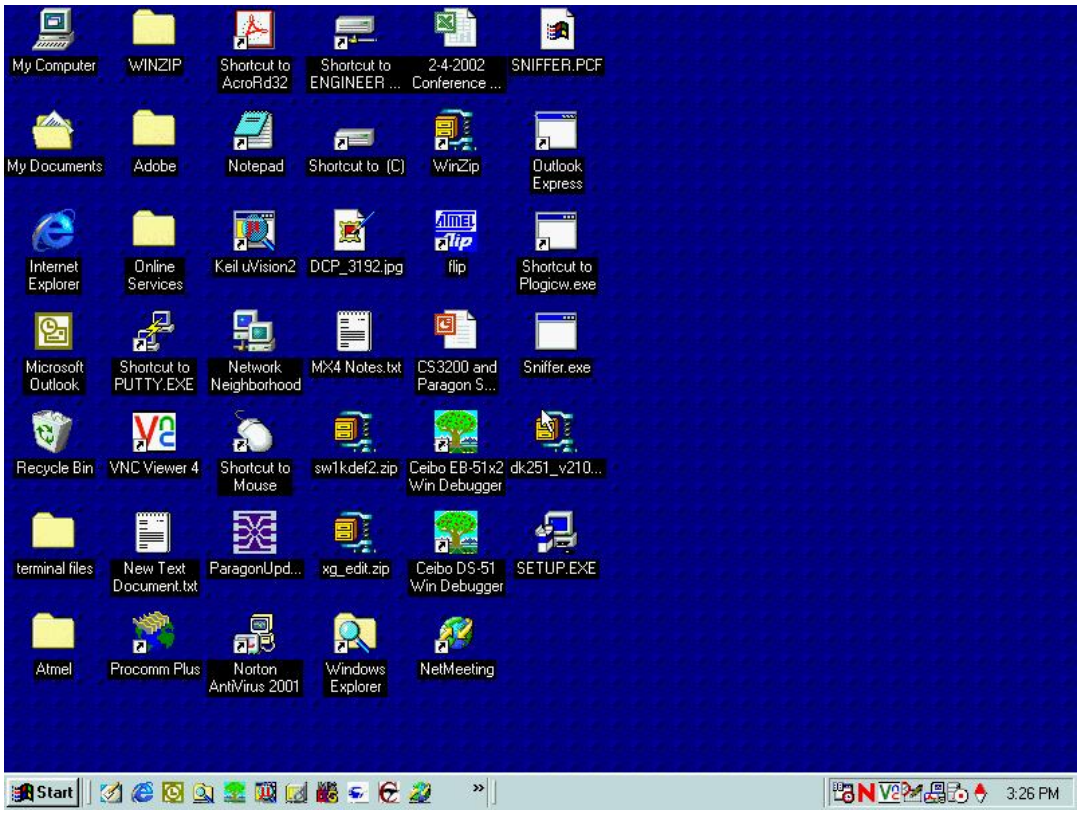
RRC Full Screen Mode

Full screen mode removes the surrounding RRC graphical interface and your local desktop area, filling your screen with the video from the target server. Your screen's resolution will be adjusted to match the resolution of the target server (provided your graphics system supports it). If your graphics system does not support the resolution of the target system, you will be unable to activate full screen mode and a message will appear requesting that you change your video resolutions first.

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

Activate full screen mode in one of the following ways once you are connected to a target:

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

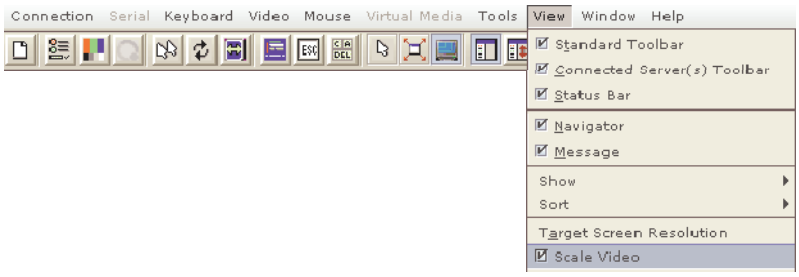


Scaling

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

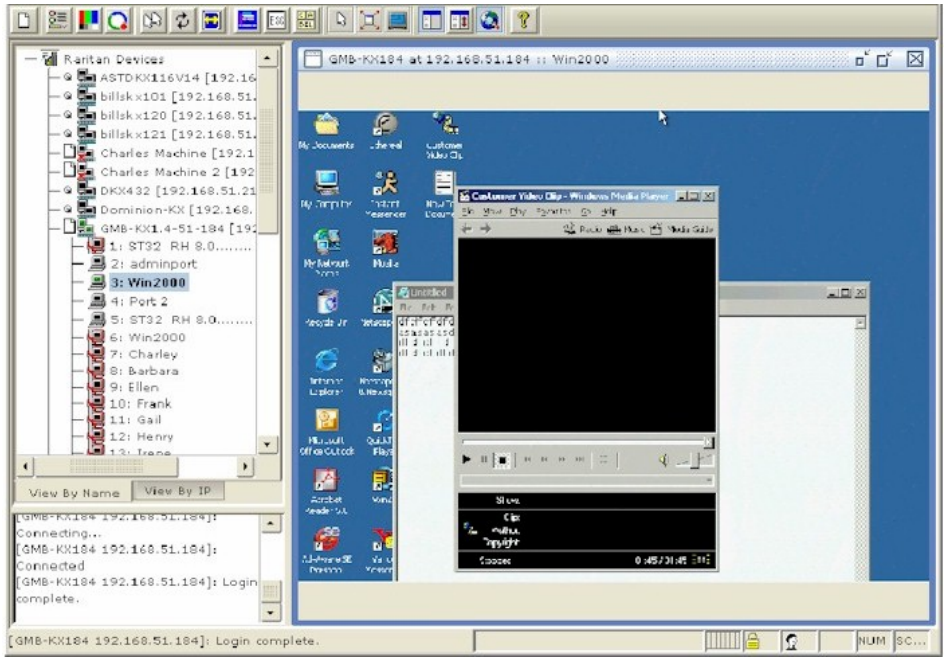
To activate Scale Video mode, do one of the following:

- Choose View > Scale Video.



- Click the Scaling button on the toolbar.

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



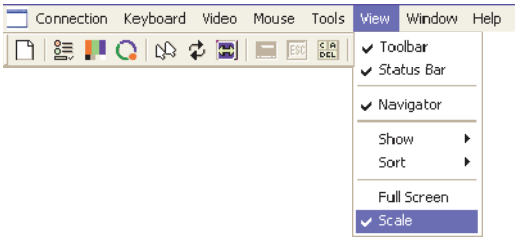
Note: Enabling Scale Video will scale the complete target video image to fit the remote desktop area as it grows or shrinks. You can combine this setting with target screen resolution for a full page affect on targets with a higher resolution than your desktop.

RRC Scaling (Shared)

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

To activate Scale Video mode, do one of the following:

- Choose View > Scale.



- Click the Scaling button on the toolbar.

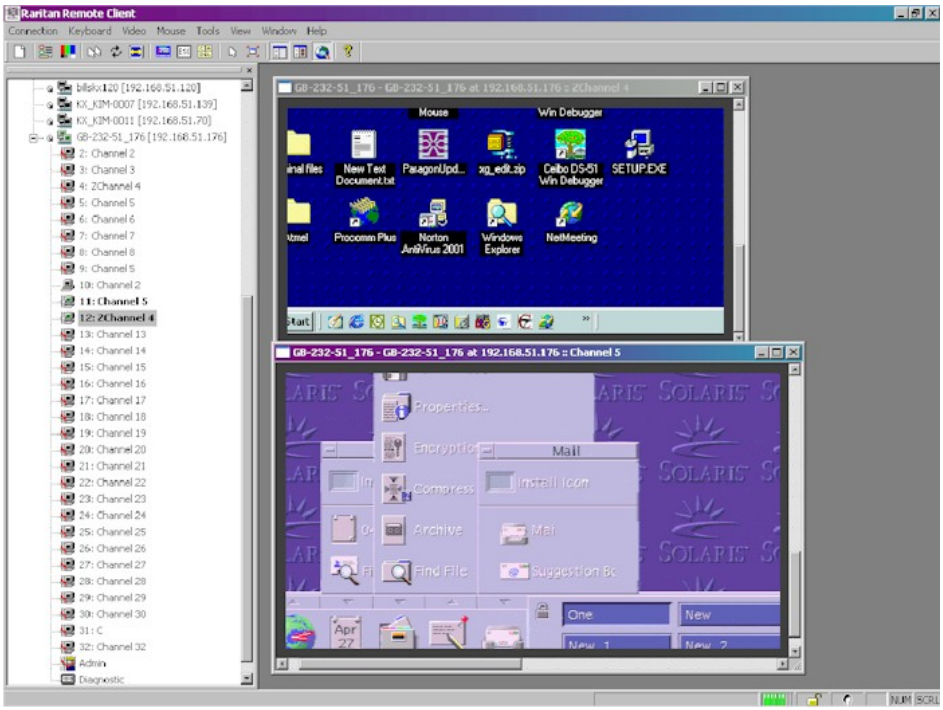
To exit this mode and return the target window to its previous size, choose Scale on the View menu or click the Scaling button once again.

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

Auto-Scroll

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

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



Shortcut Menu

To access the shortcut menu, use either the default keyboard combination of Ctrl+Left Alt+M or the keyboard combination you assign. See ***Changing the Shortcut Menu Keyboard Combination*** (on page 88) for more information.

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

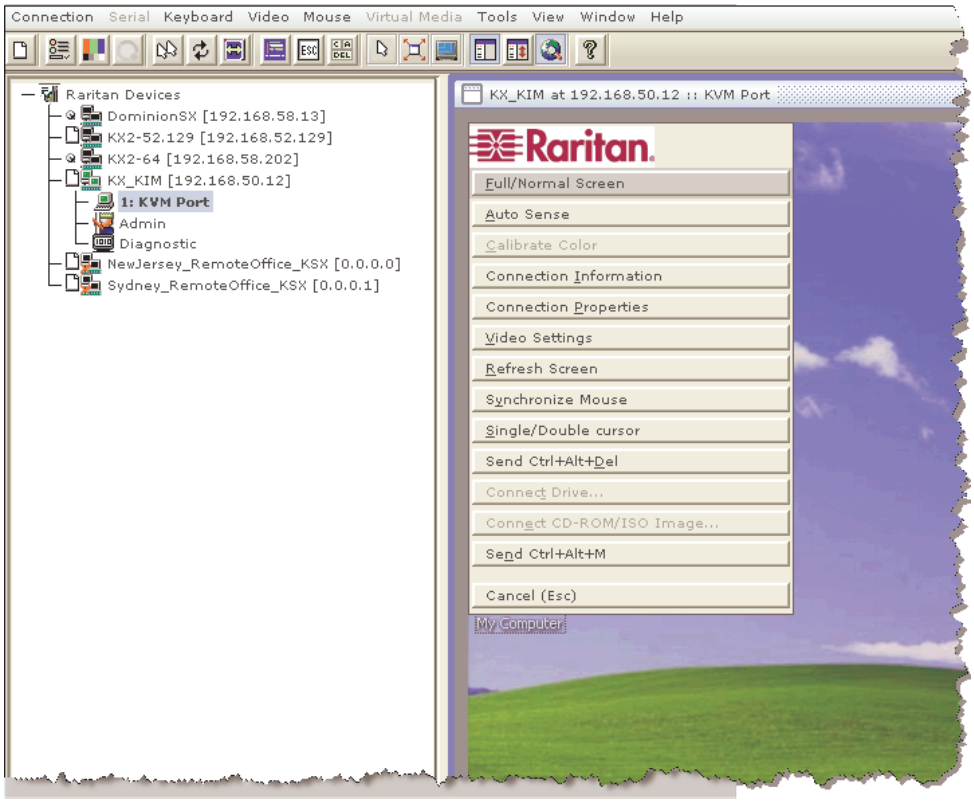
Note: You must use the Left Alt key on your keyboard when using the Ctrl+Left+Alt combination.

To	Press Ctrl+Left Alt+M+_
Toggle between Full/Normal screen mode*	F
Perform video autosensing**	A
Display connection information*	I
Display or set connection properties*	P
Display or set video settings*	V
Refresh the page	R
Color calibrate**	C
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 a dialog or menu without altering the keyboard state	Esc

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

** If Full Screen mode is active, executing this command will automatically end Full Screen mode only in RRC.

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

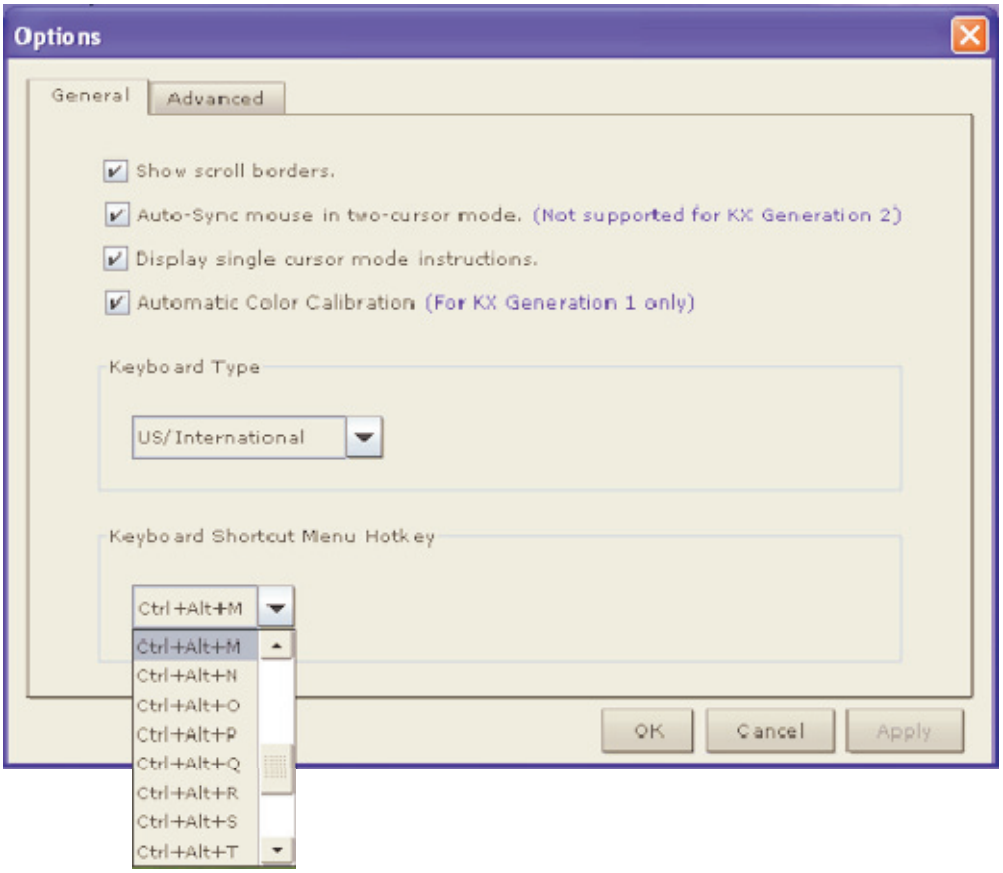


Changing the Shortcut Menu Keyboard Combination

➢ ***To change the keyboard combination that opens the shortcut menu used in MPC, do the following:***

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

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



Keyboard Macros

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

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

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

Building a Keyboard Macro

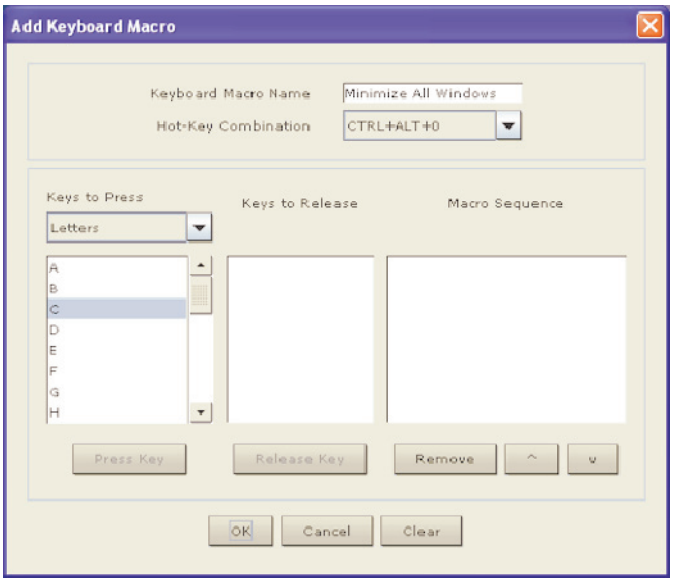
➢ ***To build a macro:***

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

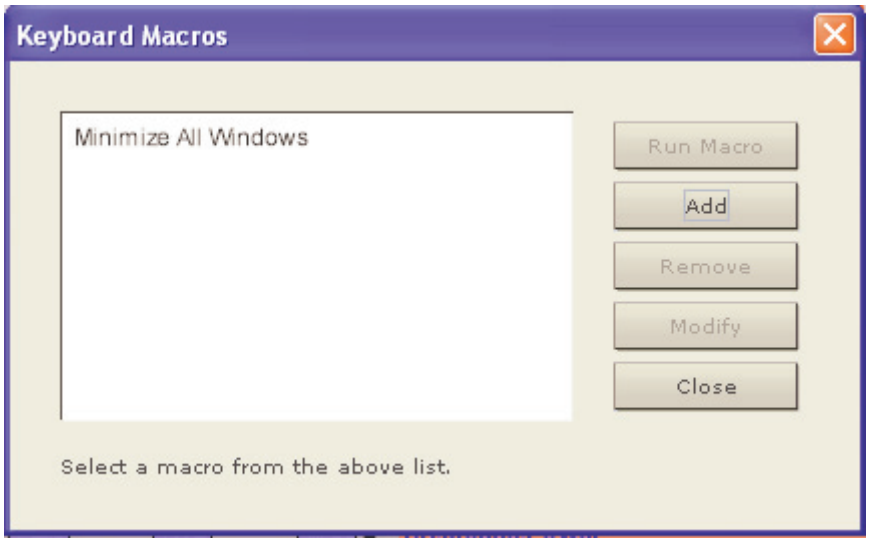
      As each key is selected, it will appear in the Keys to Release field. For example, select the Windows key and the letter D key. When these keys are selected, the macro will be executed. Add a key release attribute to the macro if needed (see next step).

d. In the Keys to Release field, you can define the keys you want released in order to run the macro. For example, specify that the keys to be pressed must also be released in order for the macro to be executed. Select the keys in the order by which they are to be released. Click Release Key after each selection.

e. Review the Macro Sequence field to be sure the macro sequence is defined correctly. The contents of this field are automatically generated and are based on the selections made in the Keys to Press and Keys to Release fields. To remove a step in the sequence, select it and click Remove. To change the order of steps in the sequence, click on the step and then click the up or down arrow buttons to reorder them as needed.



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



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

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

Running a Keyboard Macro

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

Run a Macro from the Menu Bar

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

Run a Macro Using a Keyboard Combination

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

Ctrl+Alt+Del Macro

Due to its frequent use, a Ctrl+Alt+Delete macro, used to reboot the target computer, has been preprogrammed into MPC and RRC. Clicking on the Ctrl+Alt+Delete button  in the toolbar sends this key sequence to the server or to the KVM switch to which you are currently connected.

In contrast, if you were to physically press the Ctrl+Alt+Del keys while using MPC or 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.

Common Hot Key Exceptions for MPC

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

Hot Key Combination	Description
Ctrl+Alt+Delete	Reboots the computer. The sequence is sent to the local system and the Windows Security (Task Manager, Shutdown, and so on) dialog is displayed.
Ctrl+Left Alt+M	Brings up the ***shortcut menu*** (on page 87).
Print Scrn	Treated locally and copies the page to the clipboard.

Following are limitations to specific keyboards and hot key combinations:

Hot Key Combination	Description
Alt Gr	Because of a limitation in the Java Runtime Environment (JRE), Fedora, Linux, and Solaris clients receive an invalid response from Alt Gr on United Kingdom and US International language keyboards. Fedora, Linux, and Solaris do not pick up events for the Alt Gr key combination for Java 1.4.2 or 1.5. Java 1.6 appears to improve on this, although the keyPressed and keyReleased events for Alt Gr still identify it as an "unknown key code". Further, a key pressed in combination with Alt Gr (such as on the UK keyboard Alt Gr-4, which is the Euro symbol), will only generate a keyTyped followed by a keyReleased event for that value without a keyPressed event. Java 1.6 improves upon this by filling in the keyPressed event as well.
Alt+SysRq+[key]	Since the SysRq keyboard stroke is used by some operating systems as a print shortcut, the Alt + SysRq + [key] combination is supported only as a macro when using DKX with RRC and MPC to a Linux target.

Common Hot Key Combinations for RRC

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

Hot Key Combination	Description
Ctrl+Alt+Delete	Reboots the computer. The sequence is sent to the local system and the Windows Security (Task Manager, Shutdown, and so on) dialog is displayed.
Ctrl+Num Lock	This toggles the state of the Num Lock light if the Num Lock state on the local system is not the same as the target system.

Hot Key Combination	Description
Ctrl+Caps Lock	This toggles the state of the Caps Lock light if the Caps Lock state of the local system is not the same as the target system.
Ctrl+Scroll Lock	This toggles the state of the Scroll Lock light if the Scroll Lock state of the local system is not the same as the target system.
Ctrl+Left Alt+M	Brings up the ***shortcut menu*** (on page 87).
Print Scrn	Treated locally and copies the page to the clipboard.

Following are limitations to specific keyboards and hot key combinations:

Hot Key Combination	Description
Alt+SysRq+[key]	Since the SysRq keyboard stroke is used by some operating systems as a print shortcut, the Alt + SysRq + [key] combination is supported only as a macro when using DKX with RRC and MPC to a Linux target.

Raritan Remote Client Sun Hot Key Combination Equivalents

The following keys are commands specific to the special keys on the Sun keyboard. Use RRC hot key combinations in their place.

Sun key	RRC
Again	Ctrl+Alt+F2
Props	Ctrl+Alt+F3
Undo	Ctrl+Alt+F4
Front	Ctrl+Alt+F5
Copy	Ctrl+Alt+F6
Open	Ctrl+Alt+F7
Paste	Ctrl+Alt+F8
Find	Ctrl+Alt+F9
Cut	Ctrl+Alt+F10

Sun key	RRC
Help	Ctrl+Alt+F11
Mute	Ctrl+Alt+F12
Compose	Ctrl+ Alt + KPAD *
VOL+	Ctrl + Alt + KPAD +
VOL-	Ctrl + Alt + KPAD -
Stop+A	Pause/Break+A
Stop	No key combination
Power	No key combination

Keyboard Type

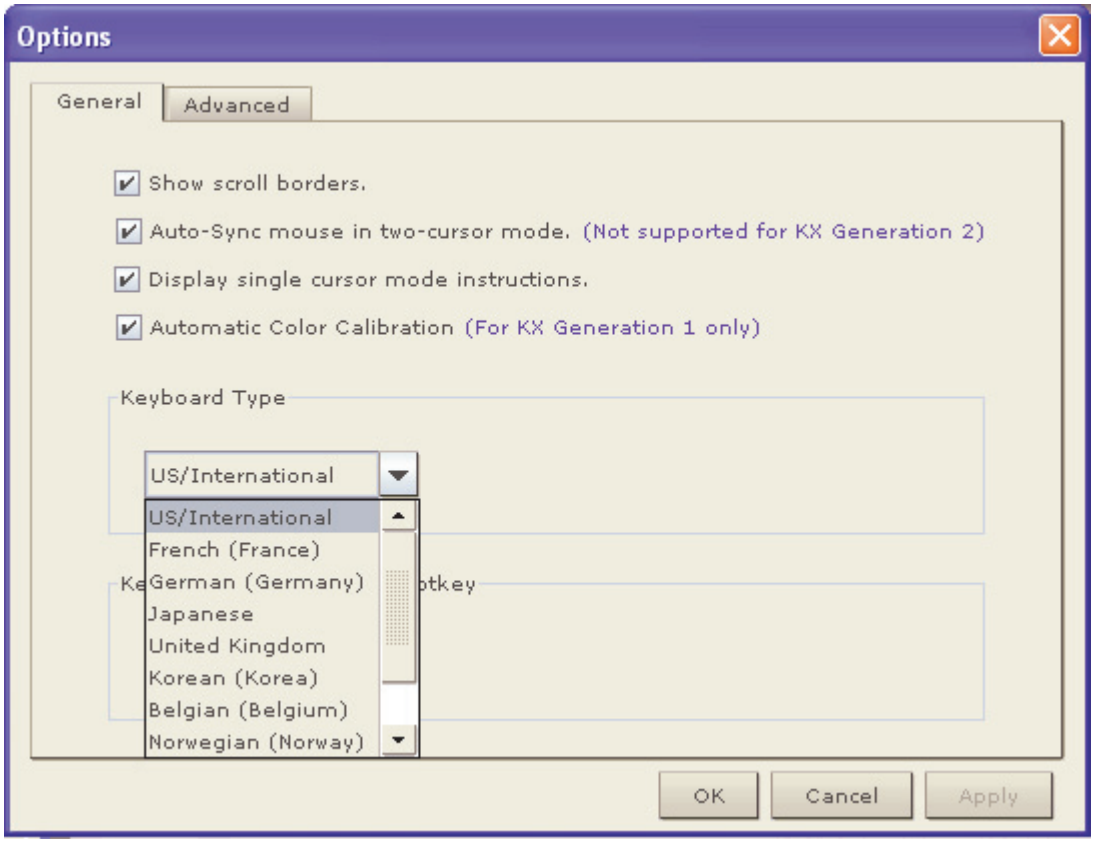
Specifying a Keyboard Type in MPC

MPC will not autodetect the type of keyboard you use, so you must specify your keyboard type to ensure accurate keyboard mapping. Options include US/International, French, German, Japanese, UK English, Korean, Belgian, and Norwegian.

➢ ***To specify a keyboard type:***

1. On the Tools menu, choose Options. The Options dialog will appear.
2. Click on the Keyboard Type drop-down and select your keyboard type from the list.

3. Click OK.



Windows Key in MPC

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

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

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

Keyboard Limitations

Japanese Kanji Keyboards

For Kanji keyboards, when using DCIM-USBs and MPC, the remote client cannot enter EISU mode by pressing the Caps Lock key (key#30). Local port access is not affected. You can access the DCIM-USBs using RRC or using the keyboard macro Shift + Caps Lock in MPC.

Language Configuration on Linux

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

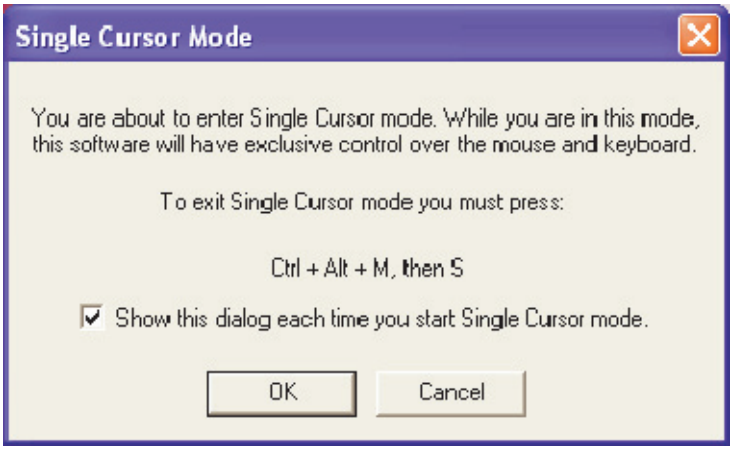
Language	Configuration method
US Intl	Default
UK	System Settings (Control Center)
French	Keyboard Indicator
German	System Settings (Control Center)
Norwegian	Keyboard Indicator
Swedish	Keyboard Indicator
Danish	Keyboard Indicator
Japanese	System Settings (Control Center)
Korean	System Settings (Control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

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

Single Mouse Mode/Dual Mouse Mode

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

On fast LAN connections, you may want to disable the mouse pointer and view only the target server's pointer. To toggle between these two modes, choose Single/Double Cursor on the shortcut menu to enable single/double cursor mode. Alternatively, click the Single Mouse Pointer icon in the toolbar or choose Mouse > Single Cursor Mode.



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

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

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

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 choosing Options from the Tools menu and clicking on the checkbox before Auto-Sync mouse in two-cursor mode.

Mouse Synchronization Options

In addition to synchronizing mouse pointers or toggling between single and double cursor mode, the Mouse menu provides three options for synching pointers when in Dual Cursor mode:

Menu Option	Description
Absolute	When connected to selected Dominion devices and targets with USB ports, the application will use absolute coordinates to keep the pointers in sync. Note: The absolute mouse setting requires a USB target system and is the recommended mouse setting for KX101.
Intelligent	Under certain conditions, the application can detect the target mouse settings and synchronize the mouse pointers accordingly, accelerating the mouse on the target device. See ***Intelligent Mouse Synchronization Conditions*** (see "Intelligent Mouse Synchronization" on page 101) for more details.
Standard	This is the standard mouse synchronization algorithm. For the proper target mouse settings, see the user guide of your Raritan device.

Note that the intelligent and standard mouse are only available to users working on Dominion devices.

Intelligent Mouse Synchronization

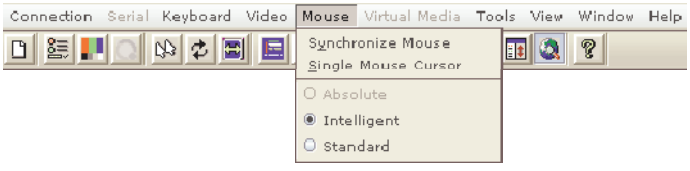
The Intelligent Mouse Synchronization command, available on the Mouse menu, automatically synchronizes mouse cursors during moments of inactivity. For this to work properly, however, the following conditions must be met:

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

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

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

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



Connection and Video Properties

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

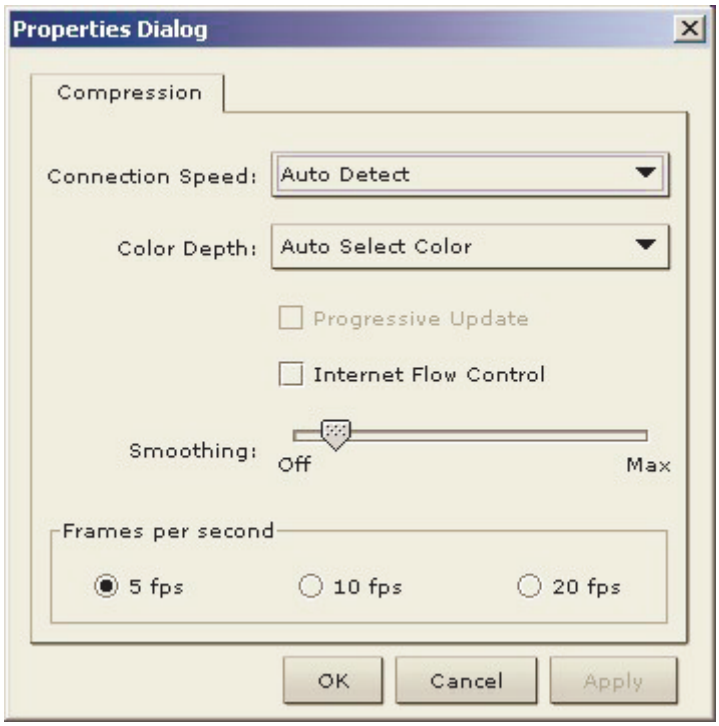
The parameters discussed in this section can be optimized in the Connection Properties dialog and Video Settings dialog to suit your requirements for different operating environments.

MPC Connection and Video Properties

MPC Connections

➢ ***To set connection properties in MPC:***

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



2. Connection Speed: Use this setting to manually adjust the connection speed to accommodate bandwidth constraints. IP-Reach and Dominion can automatically detect available bandwidth and not limit bandwidth use, but you can also adjust this usage according to your needs. Depending on the Raritan device in use, different options may be available.
   - Auto Detect
   - 1G Ethernet
   - 100mb Ethernet
   - 10mb Ethernet
   - 1.5mb (Max DSL/T1)
   - 1mb (Fast DSL/T1)
   - 512 kb (Medium DSL/T1)
   - 384 kb (Slow DSL/T1)
   - 256 kb (Cable)
   - 128 kb (Dual ISDN)
   - 56 kb (ISP Modem)
   - 33 kb (Fast Modem)
   - 24 kb (Slow Modem)
3. Color Depth: IP-Reach and Dominion can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths. Select from among the options in the drop-down list (depending on the Raritan device in use, different options may be available):
   - 15-bit RGB Color
   - 8-bit RGB Color
   - 4-bit Color
   - 4-bit Gray
   - 3-bit Gray
   - 2-bit Gray
   - Black and White
   - For information on Progressive Update, Internet Flow Control, Smoothing (15-bit mode only), and Frames per second (MPC only), refer to ***Connection Profiles*** (on page 53).

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

4. Click OK to change the Connection Properties.

MPC Video Properties

Refreshing Video Settings

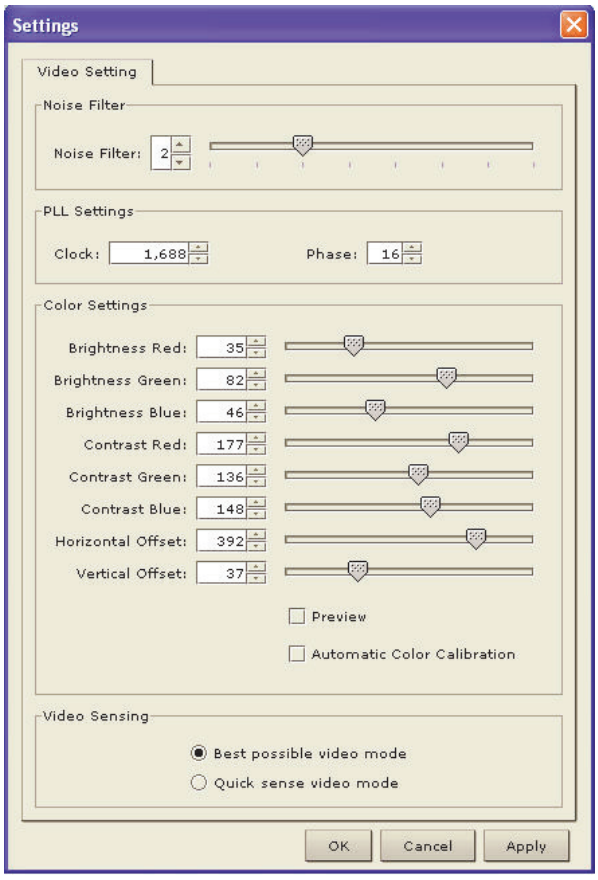
Video settings can be refreshed in several ways:

- Using Video > Refresh Screen.
- Directing IP-Reach or Dominion to automatically detect the video settings (Video > Auto-sense Video Settings).
- Using the ***Color Calibration*** (on page 120) command to calibrate the video, thereby enhancing the colors that are displayed.
- Changing the settings from the Video Settings dialog.

Change RRC Video Settings

➢ ***To change the video settings:***

1. Choose Video > Video Settings or click the Video Settings button in the toolbar. The Settings dialog appears and you can update the desired settings.



2. Noise Filter: IP Reach and Dominion can filter out the electrical interference of video output from graphics cards. This feature optimizes picture quality and reduces bandwidth. Higher settings transmit variant pixels only if a large color variation exists in comparison to the neighboring pixels. However, setting the threshold too high can result in the unintentional filtering of desired page changes. Lower settings transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.

   Note: 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.

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

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

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

4. Color Settings: These settings control the brightness, contrast, and positioning of the target server display.
   - Brightness Red: Controls the brightness of the red signal; range is 0 - 127.
   - Brightness Green: Controls the brightness of the green signal; range is 0 - 127.
   - Brightness Blue: Controls the brightness of the blue signal; range is 0 - 127.
   - Contrast Red: Controls the red signal contrast; range is 0 - 255.
   - Contrast Green: Controls the green signal contrast; range is 0 - 255.
   - Contrast Blue: Controls the blue signal contrast; range is 0 - 255.

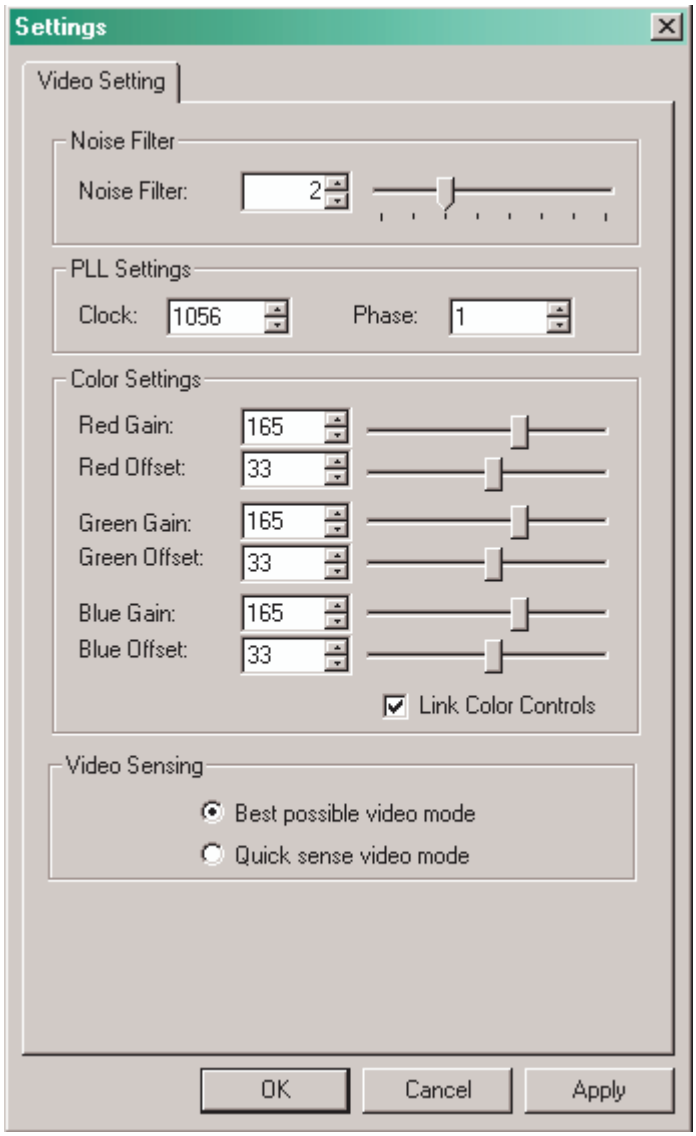
- Horizontal Offset: Controls the horizontal positioning of the target server display on your monitor; range is 0 - 512.
- Vertical Offset: Controls the vertical positioning of the target server display on your monitor; range is 0 - 128.

5. To preview the change prior to making the selection, check the Preview checkbox.
6. Check the Automatic Color Calibration checkbox to enable this feature.
7. Select the video sensing mode:
   - Best possible video mode: IP-Reach or Dominion will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.
   - Quick sense video mode: Selecting this option will cause IP-Reach or Dominion 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.
8. Click OK to change the Video Settings.

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 page.

Video Settings (Generation 1 Equipment Only)

1. Choose Video > Video Settings or click the Video Settings button  in the toolbar. The Settings dialog appears.



These settings can be refreshed using the Color Calibration command, described in the next section, by manually forcing IP-Reach or Dominion to autodetect the video settings (on the Video menu, click Auto-sense Video Settings), or by changing the settings in this page. After you change a value, click Apply to test the setting.

2. Noise Filter: IP-Reach or Dominion can filter out electrical interference of video output from graphics cards. This feature optimizes picture quality and reduced used bandwidth.

Note: The default Noise Filter is 4; Raritan recommends that you lower this value to 0 (zero).

- Higher: Noise Filter settings instruct IP-Reach or Dominion 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 page changes.
- Lower: Noise Filter settings instruct IP-Reach or Dominion 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.

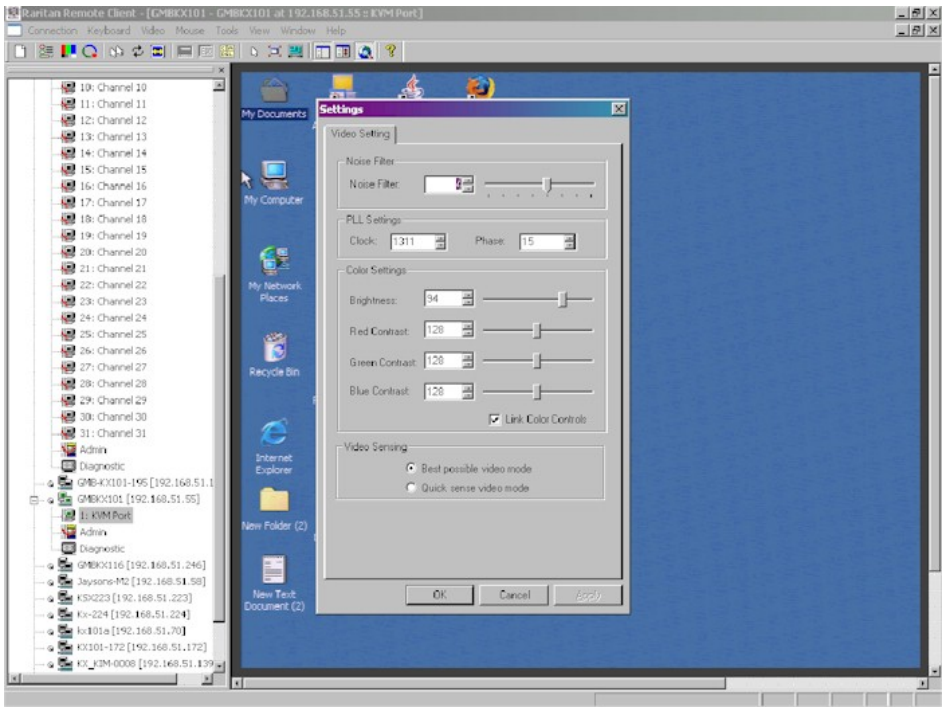
3. Analog-to-Digital Settings: The following parameters are best left to IP-Reach or Dominion to automatically detect (on the RRC Menu Bar, select Video > Auto-sense Video Settings), but a brief description of each is included here.
4. PLL Settings: If the video image looks extremely blurry or unfocused, 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 page. 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.
5. 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 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.

6. Select the video sensing option you would like to apply.
   - Best possible video mode: IP-Reach or Dominion will perform the full Auto Sense process when switching targets or target resolutions. Selecting this radio button will cause IP-Reach or Dominion to calibrate the video for the best image quality.
   - Quick sense video mode: Selecting this radio button will cause IP-Reach or Dominion 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.
7. Click OK to set Video Settings.

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 page.

Video Settings (KX101 Only)



Raritan's Dominion KX101 Color Settings window varies from those of other Dominion units.

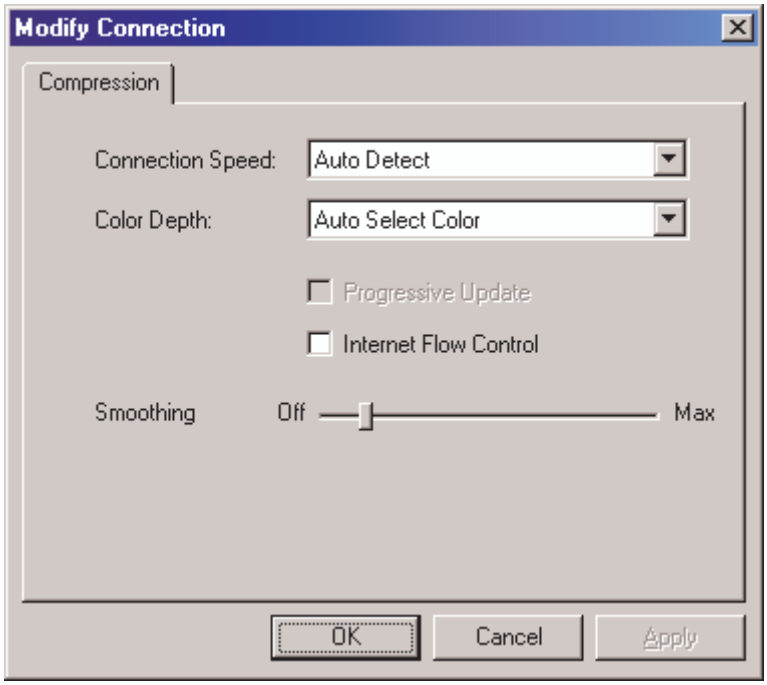
1. In the Color Settings panel, adjust the following options:
   - Brightness: Controls the backlight on your page.
   - Red Contrast: Controls the level of red tone on your page.
   - Green Contrast: Controls the level green tone on your page.
   - Blue Contrast: Controls the level of blue tone on your page.
   - Click on the Link Color Controls checkbox to make all slide adjusters move in unison when any one option is moved.
2. Click OK when finished.

RRC Connection and Video Properties

RRC Connections

➢ ***To set connection properties in RRC:***

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



2. Connection Speed: Use this setting to manually adjust the connection speed to accommodate bandwidth constraints. IP-Reach and Dominion can automatically detect available bandwidth and not limit bandwidth use, but you can also adjust this usage according to your needs. Depending on the Raritan device in use, different options may be available.
   - Auto Detect
   - 1G Ethernet
   - 100mb Ethernet
   - 10mb Ethernet
   - 1.5mb (Max DSL/T1)
   - 1mb (Fast DSL/T1)
   - 512 kb (Medium DSL/T1)
   - 384 kb (Slow DSL/T1)
   - 256 kb (Cable)
   - 128 kb (Dual ISDN)
   - 56 kb (ISP Modem)
   - 33 kb (Fast Modem)
   - 24 kb (Slow Modem)
3. Color Depth: IP-Reach and Dominion can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths. Select from among the options in the drop-down list (depending on the Raritan device in use, different options may be available):
   - 15-bit RGB Color
   - 8-bit RGB Color
   - 4-bit Color
   - 4-bit Gray
   - 3-bit Gray
   - 2-bit Gray
   - Black and White
   - For information about the Progressive Update, Internet Flow Control, and Smoothing (15-bit mode only), refer to ***Connection Profiles*** (on page 53).

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

4. Click OK to change the Connection Properties or Cancel to close the window without saving changes.

RRC Video Properties

Refresh Video Settings

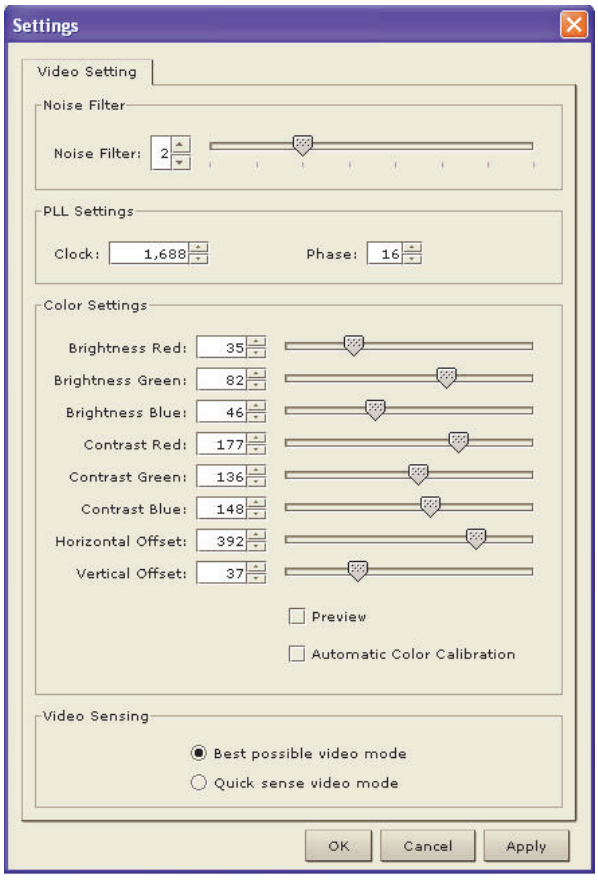
Video settings can be refreshed in several ways:

- Using Video > Refresh Screen.
- Directing IP-Reach or Dominion to automatically detect the video settings (Video > Auto-sense Video Settings).
- Using the ***Color Calibration*** (on page 120) command to calibrate the video, thereby enhancing the colors that are displayed.
- Changing the settings from the Video Settings page.

Change RRC Video Settings

➢ ***To change the video settings:***

1. Choose Video > Video Settings or click the Video Settings button in the toolbar. The Settings dialog appears. Update the desired settings.



2. Noise Filter: IP Reach and Dominion can filter out the electrical interference of video output from graphics cards. This feature optimizes picture quality and reduces bandwidth. Higher settings transmit variant pixels only if a large color variation exists in comparison to the neighboring pixels. However, setting the threshold too high can result in the unintentional filtering of desired page changes. Lower settings transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.

   Note: 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.

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

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

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

4. Color Settings: These settings control the brightness, contrast, and positioning of the target server display.
   - Brightness Red: Controls the brightness of the red signal; range is 0 - 127.
   - Brightness Green: Controls the brightness of the green signal; range is 0 - 127.
   - Brightness Blue: Controls the brightness of the blue signal; range is 0 - 127.
   - Contrast Red: Controls the red signal contrast; range is 0 - 255.
   - Contrast Green: Controls the green signal contrast; range is 0 - 255.
   - Contrast Blue: Controls the blue signal contrast; range is 0 - 255.

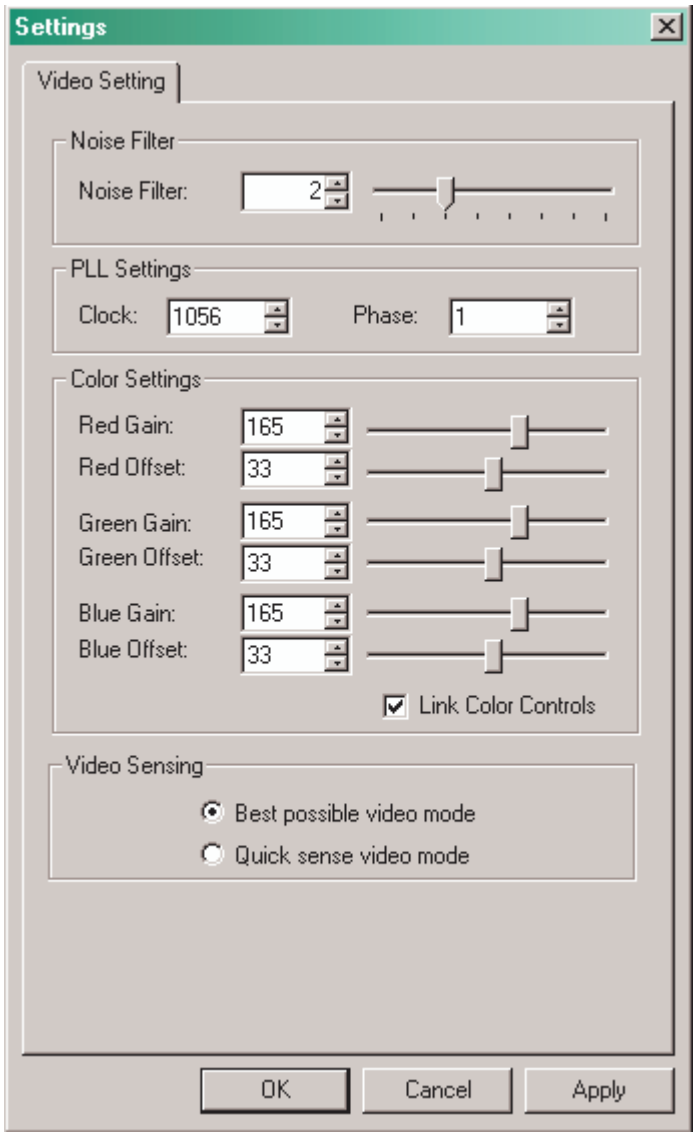
- Horizontal Offset: Controls the horizontal positioning of the target server display on your monitor; range is 0 - 512.
- Vertical Offset: Controls the vertical positioning of the target server display on your monitor; range is 0 - 128.

5. To preview the change prior to making the selection, check the Preview checkbox.
6. Check the Automatic Color Calibration checkbox to enable this feature.
7. Video Sensing: Select the video sensing mode:
   - Best possible video mode: IP-Reach or Dominion will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.
   - Quick sense video mode: Selecting this option will cause IP-Reach or Dominion 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.
8. Click OK to change the Video Settings.

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 page.

Video Settings (Generation 1 Equipment Only)

1. Choose Video > Video Settings or click the Video Settings button  in the toolbar. The Settings dialog appears.



These settings can be refreshed using the Color Calibration command, described in the next section, by manually forcing IP-Reach or Dominion to autodetect the video settings (on the Video menu, choose Auto-sense Video Settings), or by changing the settings in this page. After you change a value, click Apply to test the setting.

2. Noise Filter: IP-Reach or Dominion can filter out electrical interference of video output from graphics cards. This feature optimizes picture quality and reduced used bandwidth.

Note: The default Noise Filter is 4; Raritan recommends that you lower this value to 0 (zero).

- Higher: Noise Filter settings instruct IP-Reach or Dominion 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 page changes.
- Lower: Noise Filter settings instruct IP-Reach or Dominion 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.

---

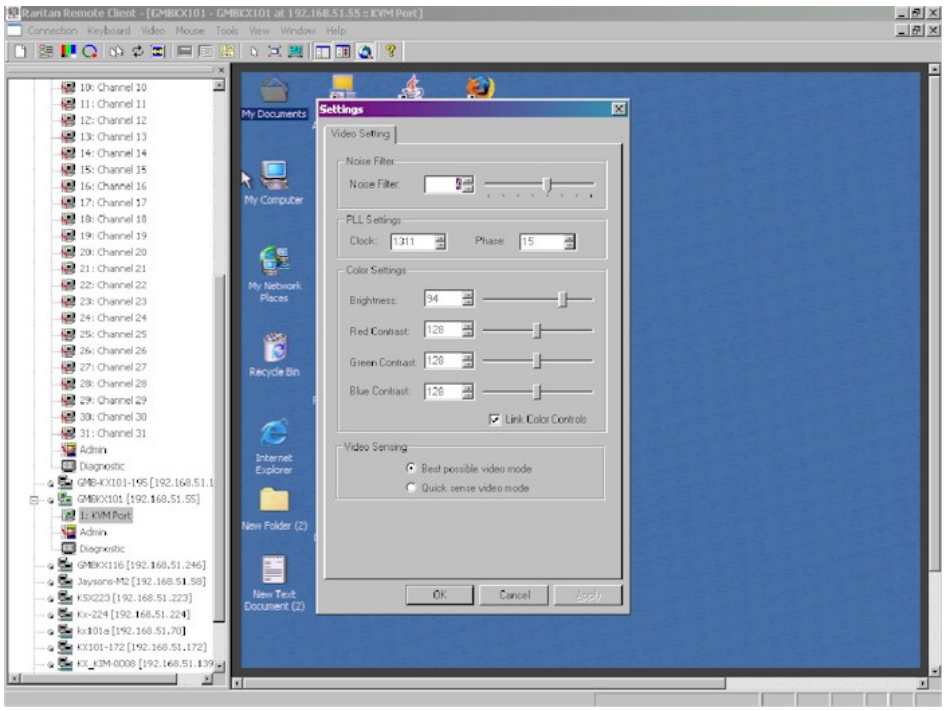
3. Analog-to-Digital Settings: The following parameters are best left to IP-Reach or Dominion to automatically detect (on the RRC Menu Bar, select Video > Auto-sense Video Settings), but a brief description of each is included here.
4. PLL Settings: If the video image looks extremely blurry or unfocused, 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 page. 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.
5. 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 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.

6. Video Sensing
   - Best possible video mode: IP-Reach or Dominion will perform the full Auto Sense process when switching targets or target resolutions. Selecting this radio button will cause IP-Reach or Dominion to calibrate the video for the best image quality.
   - Quick sense video mode: Selecting this radio button will cause IP-Reach or Dominion 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.
7. Click OK to set Video Settings.

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 page.

Video Settings in Window (KX101)



Raritan's Dominion KX101 Color Settings window varies from those of other Dominion units.

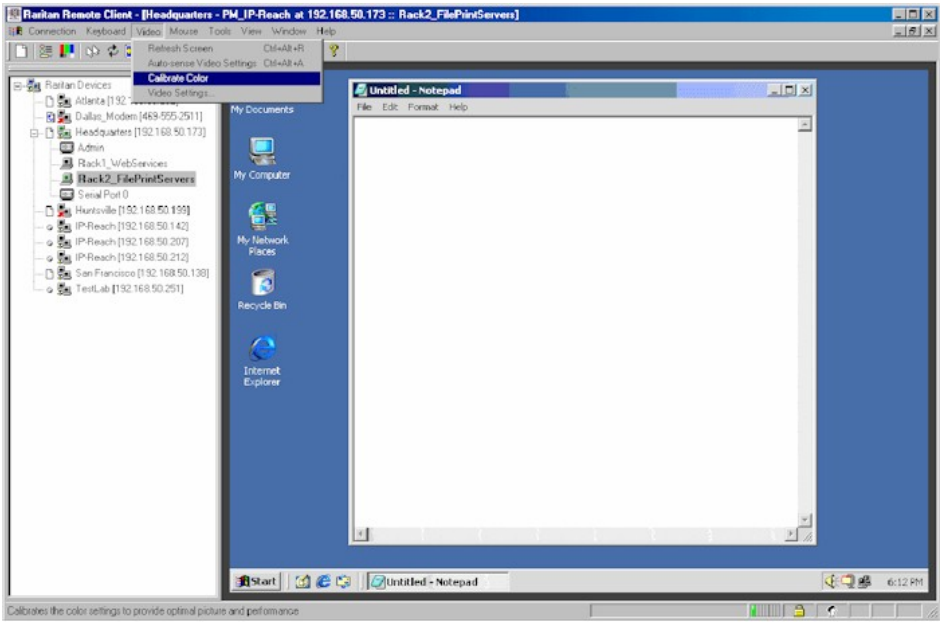
1. In the Color Settings panel, adjust the following options:
   - Brightness: Controls the backlight on your page.
   - Red Contrast: Controls the level of red tone on your page.
   - Green Contrast: Controls the level green tone on your page.
   - Blue Contrast: Controls the level of blue tone on your page.
   - Click on the Link Color Controls checkbox to make all slide adjusters move in unison when any one option is moved.
2. Click OK when finished.

Color Calibration

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

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

TIP: Open Microsoft Notepad and maximize the window.



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

Tip: You can also specify automatic color calibration using Tools > Options. Refer to ***General Options*** (see "General Options in MPC" on page 122) for more information.

Administrative Functions

Overview

Although your IP-Reach or Dominion device provides a remote interface to administrative functions through IP-Reach or Dominion Manager, MPC and RRC provide an interface to frequently-used administrative functions directly from its own interface. When logged into an IP-Reach or Dominion unit as an administrator, you can perform the administrative tasks discussed here.

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

Note to MPC Users

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

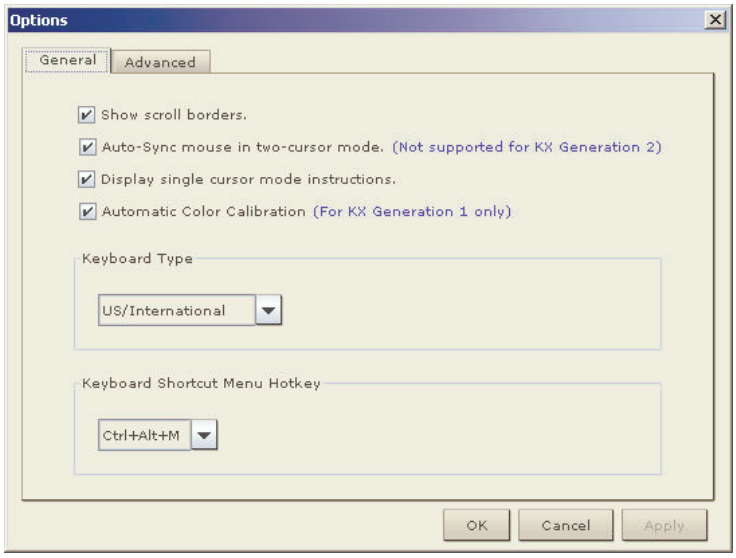
General Options

General Options in MPC

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

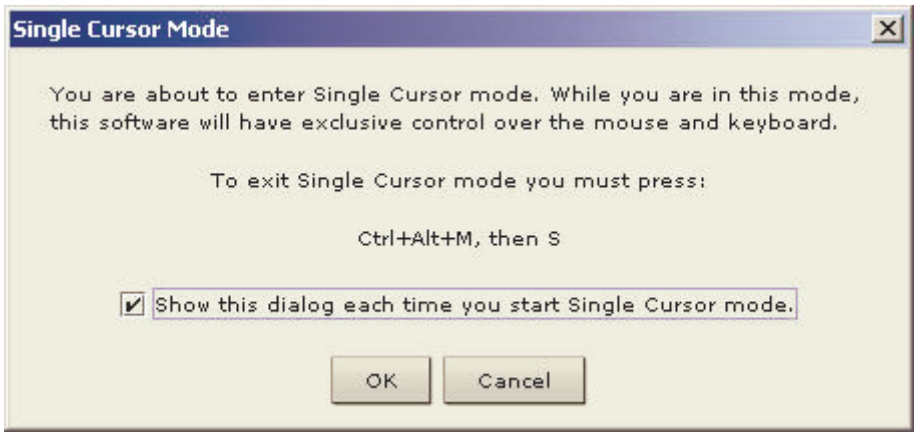
➢ ***To configure the general options in MPC:***

1. In MPC, choose Tools > Options. The Options dialog appears and displays the General tab by default.



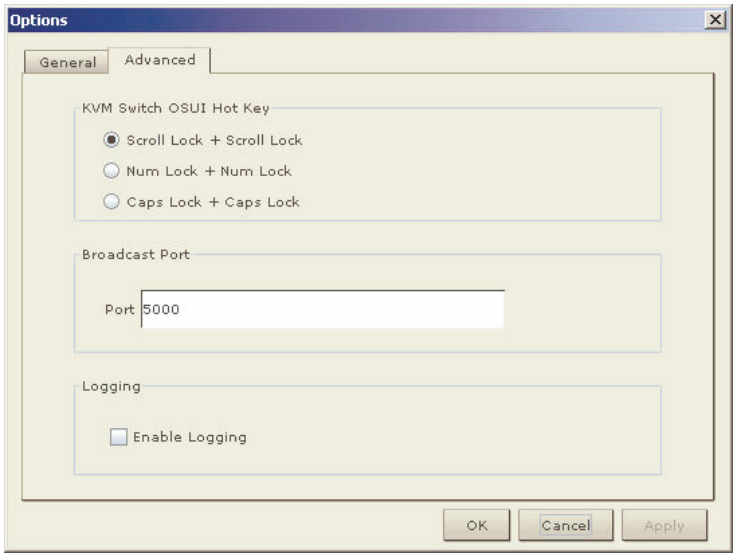
2. Select the "Show scroll borders" checkbox to view the thin scroll borders designating the autoscroll area.
3. Select the "Auto-Sync mouse in two-cursor mode" checkbox to enable automatic mouse synchronization.

4. If you select the "Display single cursor" mode instructions checkbox, the Single Cursor Mode dialog will open each time Single Cursor is enabled in the application (see ***Single Mouse Mode/Dual Mouse Mode*** (on page 99) for more information).



5. Select the Automatic Color Calibration checkbox to enable automatic color calibration. This option is available for KX generation 1 (G1) only.
6. Select the Keyboard Type from the drop-down list (depending on the Raritan device in use, different options may be available):
   - US/International
   - French (France)
   - German (Germany)
   - Japanese
   - United Kingdom
   - Korean (Korea)
   - Belgian
   - Norwegian
7. From the Keyboard Shortcut Menu HotKey drop-down, select the key combination you would like to use to invoke the ***Keyboard Shortcut Menu*** (see "Shortcut Menu" on page 87).

8. For advanced options, open the Advanced tab.



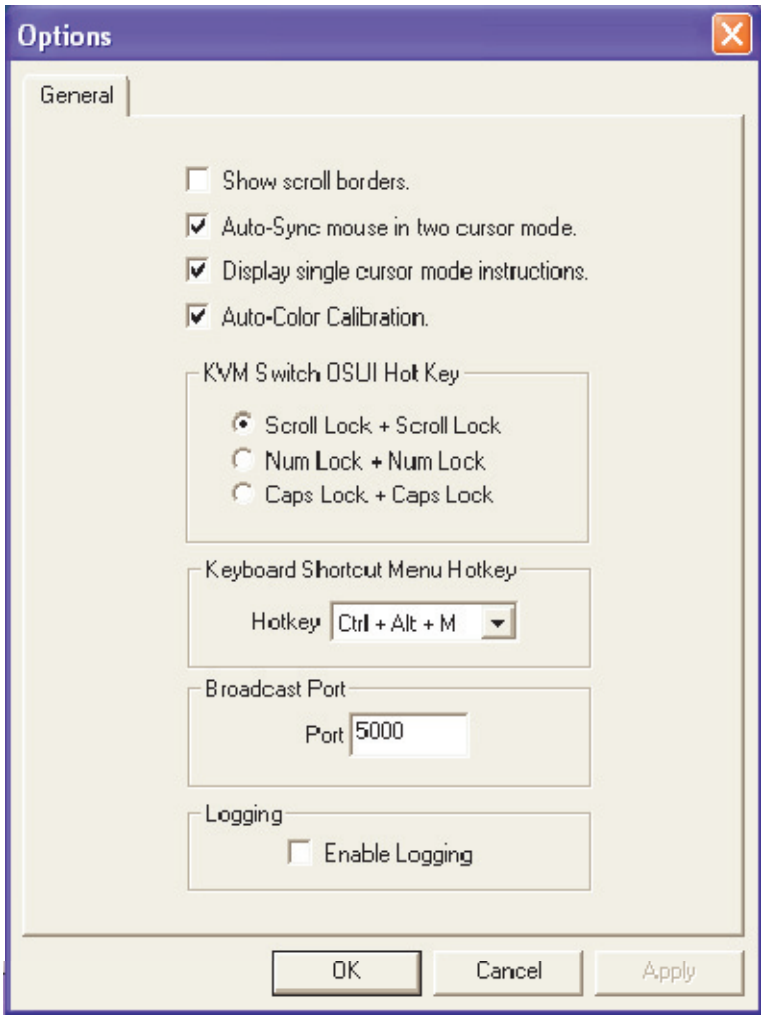
9. From the KVM Switch OSUI Hot Key section, select the hot key to use when switching between target server displays.
10. For the Broadcast Port, type the broadcast port number in the Port field if you want to use a port other then 5000.
11. Select the Enable Logging checkbox only if directed to by Technical Support. This option creates a log file in your home directory.
12. Click OK when finished. Click Apply any time while making selections to apply it.

General Options in RRC

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

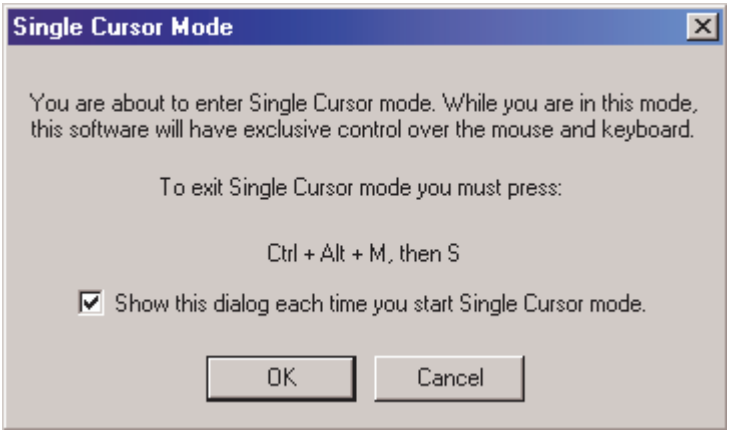
➢ ***To configure the general options in RRC:***

1. In RRC, choose Tools > Options to open the Options dialog.



2. Select the "Show scroll borders" checkbox to view the thin scroll borders that show the Auto-Scroll area.
3. Select the "Auto-Sync mouse in two cursor mode" checkbox to enable Automatic Mouse Synchronization.

4. If you select the "Display single cursor mode instructions" checkbox the Single Cursor Mode dialog will open each time Single Cursor is enabled in the application (see ***Single Mouse Mode/Dual Mouse Mode*** (on page 99) for more information).



5. Select Auto-Color Calibration to enable it.
6. In the KVM Switch OSUI Hot Key panel, select the radio button next to the hot key combination you would like to use.
7. In the Keyboard Type panel, click on the drop-down arrow and click on your keyboard choice.
8. In the Broadcast Port panel, type the broadcast port number in the Port field.
9. Click OK when finished. Click Apply any time during your selection to apply an option you have chosen.

Upgrading Device Firmware

➢ ***To update a device's firmware:***

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

Ensure that you read all instructions included in firmware ZIP files carefully before upgrading a device.

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

Changing a Password

➢ ***To update your password***

1. Connect to an IP-Reach or Dominion target by selecting it in the Navigator.
2. Highlight the target's icon in the Navigator and then choose Tools > Update > User Password. The Change Password dialog appears.

3. Type your current password in the Old Password field.
4. Type the new password in the New Password field.
5. Retype the password in the Confirm New Password field.
6. When finished, click OK.

Restarting a Device

➢ ***To restart a device:***

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

Backing Up a Device Configuration

➢ ***To back up a device:***

1. Download the IP-Reach or Dominion device configuration to your local computer by selecting the device in the Navigator.
2. On the Tools menu, choose Save Device Configuration.

Restoring a Device Configuration

➢ ***To restore a device configuration:***

1. Upload the archived IP-Reach or Dominion device configuration by selecting the device in the Navigator.
2. On the Tools menu, choose Restore Device Configuration.

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

Backing Up a User Configuration

➢ ***To back up a unit's user configuration:***

1. Select the device in the Navigator.
2. On the Tools menu, choose Save User Configuration.

Restoring a User Configuration

➢ ***To restore a user configuration:***

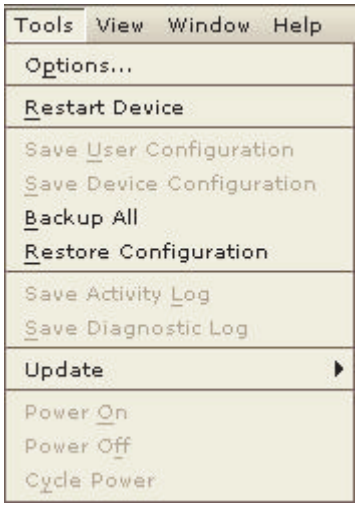
1. Upload a device's archived user configuration by selecting the device in the Navigator.
2. On the Tools menu, choose Restore User Configuration

Note: Use these commands to easily transfer user and group information from one IP-Reach or Dominion unit to another.

Backup and Restore (Dominion KX II only)

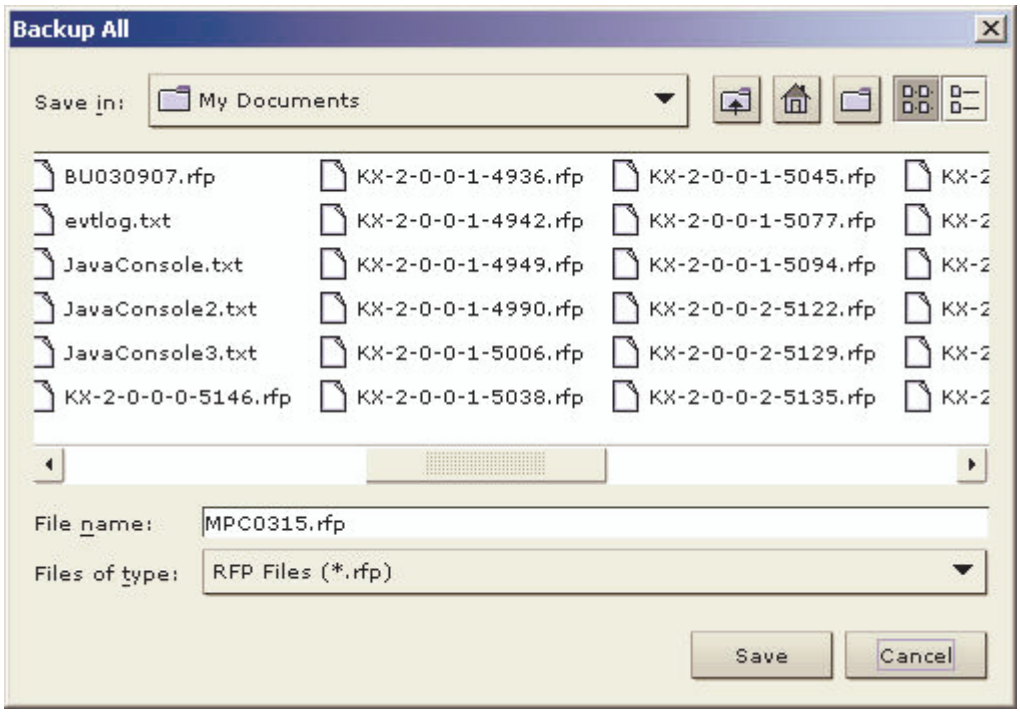
In addition to using backup and restore for business continuity purposes, you can use this feature as a time-saving mechanism. For instance, you can quickly provide access from another Dominion device to your team by backing up the user configuration settings from the device in use and restoring those configurations to the new Dominion device.

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



➢ ***To backup the entire system (both user and device configuration):***

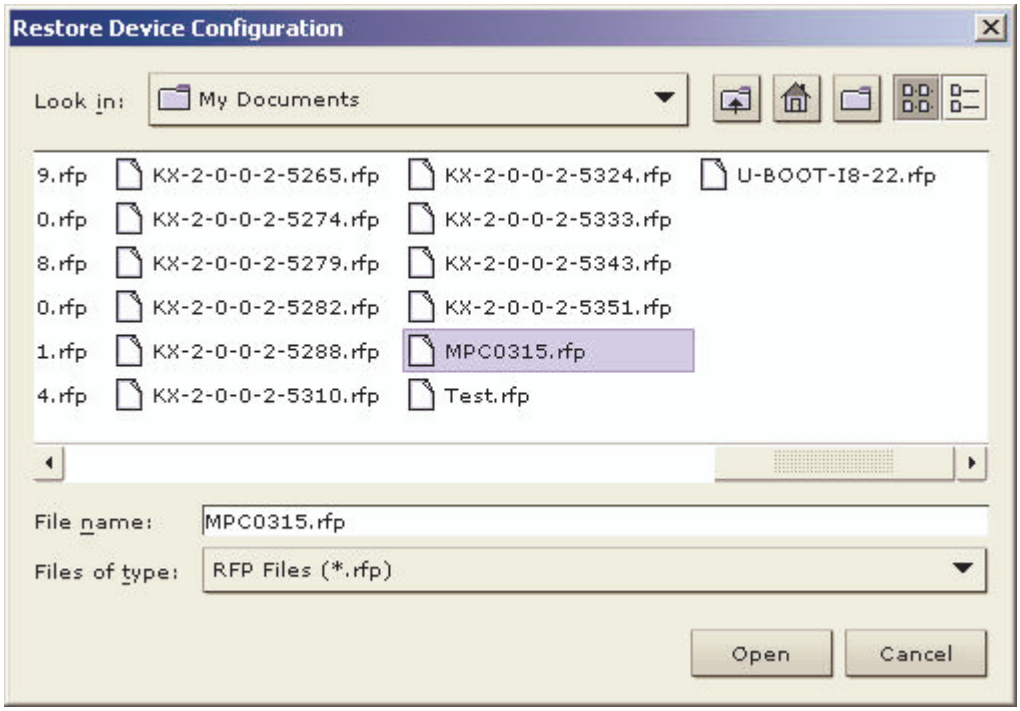
1. Choose Tools > Backup All. The Backup All dialog appears.



2. Navigate to the desired directory and give the backup file a name. (Backup files have an extension of .rfp).
3. Click Save. A message is displayed confirming the successful backup.
4. Click OK.

➢ ***To restore:***

1. Choose Tools > Restore Configuration. The Restore Device Configuration dialog appears.



2. Navigate to the appropriate directory and select the backup file.
3. Click Open. The Restore Packages dialog appears.

4. Select the type of restore you want to run:

- Full Restore: A complete restore of the entire system; generally used for traditional backup and restore purposes.
- Protected Restore: Everything is restored except device-specific information such as serial number, MAC Address, IP Address, name, port names, etc. With this option, you can setup one Dominion device and copy the configuration to multiple Dominion devices.
- Custom Restore: With this option, the following options are available. Check the appropriate checkboxes:
  - User and Group Restore: This option includes only user and group information. Use this option to quickly setup users on a different Dominion device.
  - Device Settings Restore: This option includes only device settings. Use this option to quickly copy the device information.

1. Click OK.

Log Files

Activity Log

➢ ***To download a detailed activity log for review or troubleshooting:***

1. Select the device in the Navigator.
2. On the Tools menu, choose Save Activity Log.

Diagnostic Log (excluding Dominion KX II)

To download a detailed diagnostic log for reporting or analysis:

1. Select the device in the Navigator.
2. On the Tools menu, choose Save Diagnostic Log.

Broadcast Port

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

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

1. Select the device in the Navigator.
2. On the Tools menu, choose Options. The Options dialog appears.

3. In the Broadcast Port field, type the new port number in the Port field and then click OK.

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

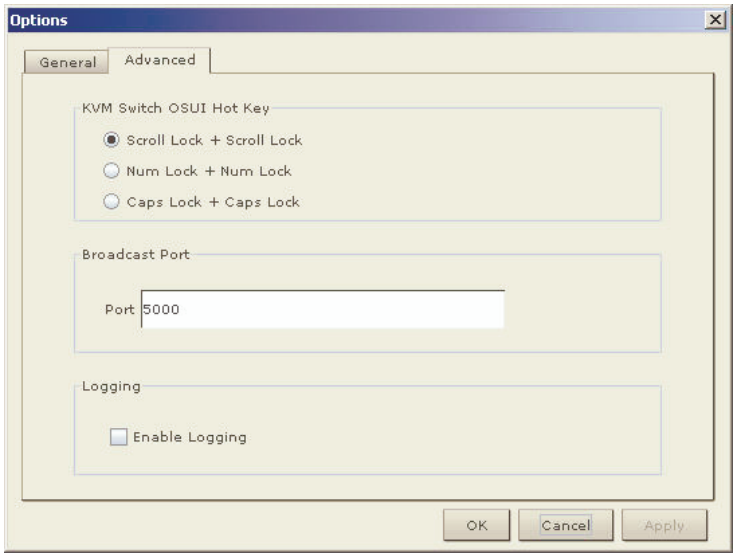
MPC Broadcast Port

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

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

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

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



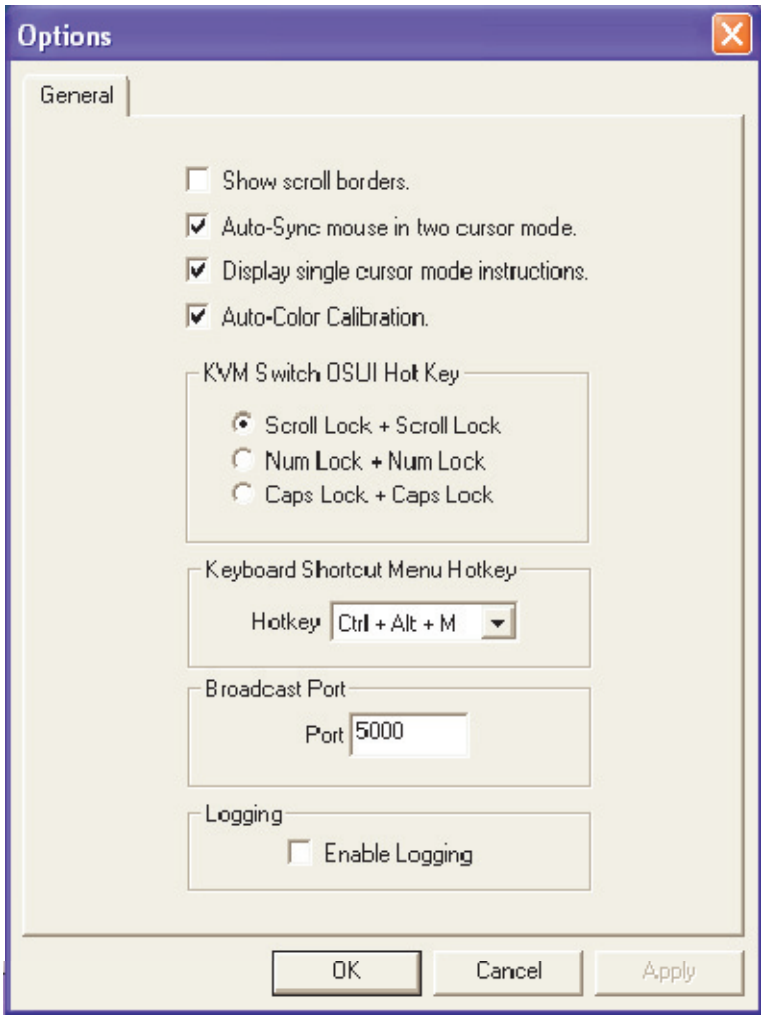
RRC Broadcast Port

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

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

1. Select the device in the Navigator.
2. On the Tools menu, choose Options. The Options dialog appears.
3. In the Broadcast Port field, type the new port number in the Port field and then click OK.

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



Remote Power Management

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

- Power On
- Power Off
- Cycle Power

➢ ***To change the power status of a target:***

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

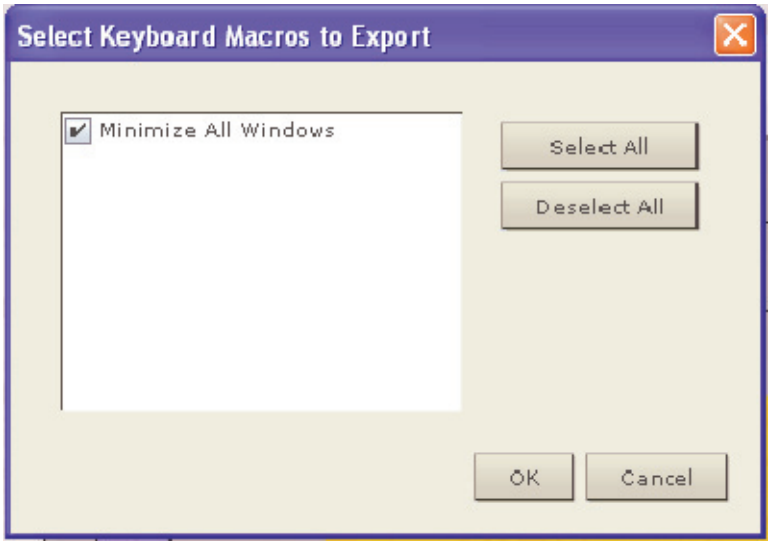
Import/Export Keyboard Macro Definitions

Import/Export MPC Keyboard Macros

The functions contained in this section describe how to exchange keyboard macro definitions between users using import and export functions. The primary purpose of this function is to exchange data between copies of MPC.

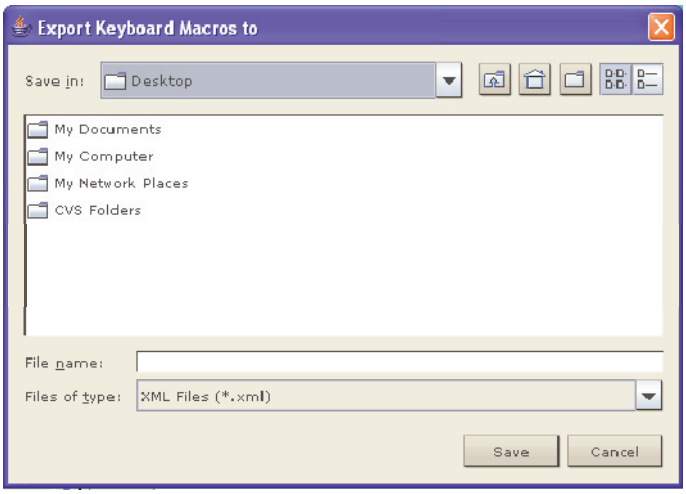
➢ ***To export MPC macros:***

1. Choose Tools > Export Macros to open the Select Keyboard Macros to Export dialog.



2. Select the macros to be exported by checking their corresponding checkbox or using the Select All or Deselect All options.
3. Click OK. The selected macro file(s) will be moved to your desktop (by default).

   A dialog from which you can locate and select the macro file will then appear. By default, the macro will exist on your desktop.
4. Locate the macro file, click on it to select it and then click Save. If the macro already exists, you will receive an alert message. Select Yes to overwrite the existing macro or No to close the alert without overwriting the macro.



➢ ***To import MPC macros:***

1. Choose Tools > Import Macros to open the Import Macros dialog. By default, the macro will exist on the desktop.
2. Click on the macro file and click Open to import the macro.
   a. If too many macros are found in the file, an error message will be displayed and the import will terminate once OK is selected.
   b. If the import fails, an error dialog will open and will display a message regarding why the import failed. Select OK to continue the import without importing the macros that cannot be imported.
3. Select the macros to be imported by checking their corresponding checkbox or using the Select All or Deselect All options.
4. Click OK and the import will begin.
   a. If a duplicate macro is found, the Import Macros dialog will appear. Do one of the following:

- Click Yes to replace the existing macro with the imported version.
- Click Yes to All to replace the currently selected and any other duplicate macros that are found.
- Click No to keep the original macro and proceed to the next macro
- Click No to All keep the original macro and proceed to the next macro. Any other duplicates that are found will be skipped as well.
- Click Cancel to stop the import.
- Alternatively, click Rename to rename the macro and import it. If Rename is selected, the Rename Macro dialog will open. Enter a new name for the macro in the field and click OK. The dialog will close and the process will proceed. If the name that is entered is a duplicate of a macro, an alert will appear and you will be required to enter another name for the macro.

b. If during the import process the number of allowed, imported macros is exceeded, a dialog will open. Click OK to attempt to continue importing macros or click Cancel to stop the import process.

The macros will then be imported.

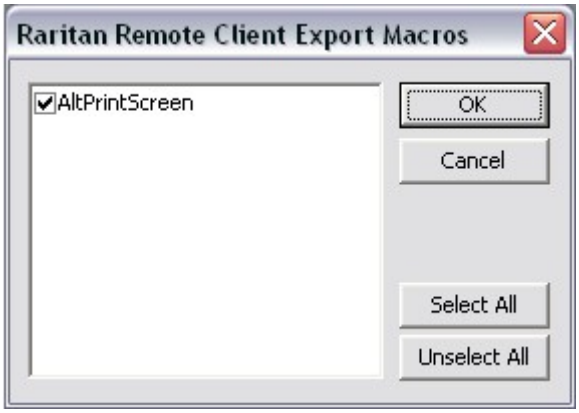
If a macro is imported that contains a hot key that already exists, the hot key for the imported macro will be discarded.

Import/Export RRC Keyboard Macros

The functions contained in this section describe how to exchange keyboard macro definitions between users using import and export functions. The primary purpose of this function is to exchange data between copies of RRC.

➢ ***To export RRC macros:***

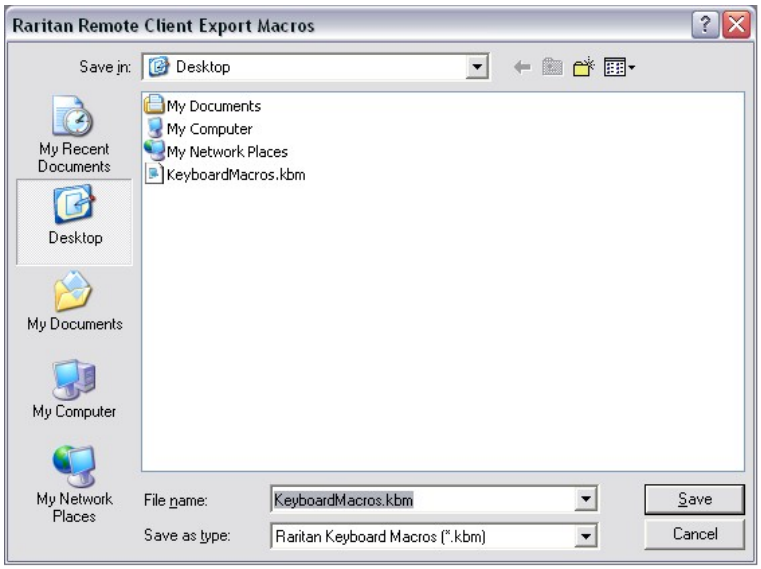
1. Choose Tools > Export Macros to open the Export Macros dialog.



2. Select the macros to be exported by checking their corresponding checkbox or using the Select All or Unselect All options.
3. Click OK. The selected macro file(s) will be moved to your desktop (by default).

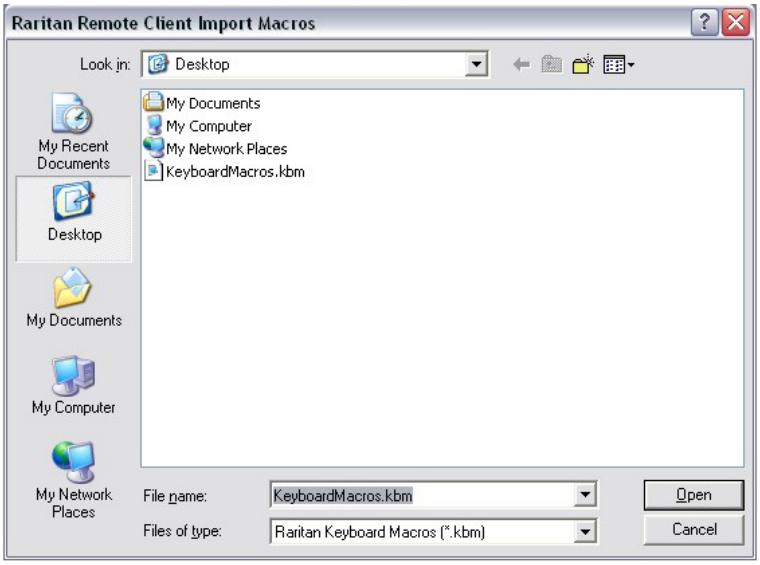
   A select dialog from which you can locate and select the macro file will then appear. By default, the macro will exist on your desktop.

4. Locate the macro file, click on it to select it and then click Save. If the macro already exists, you will receive an alert message. Select Yes to overwrite the existing macro or No to close the alert without overwriting the macro.



➢ ***To import RRC macros:***

1. Choose Tools > Import Macros to open the Import Macros dialog. By default, the macro will exist on the desktop.

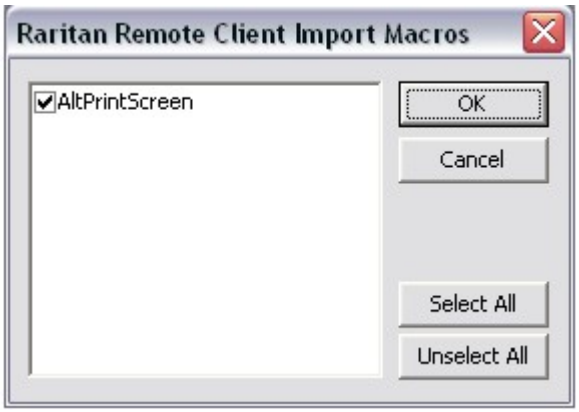


2. Click on the macro file and click Open to import the macro.

a. If too many macros are found in the file, an error message will be displayed and the import will terminate once OK is selected.

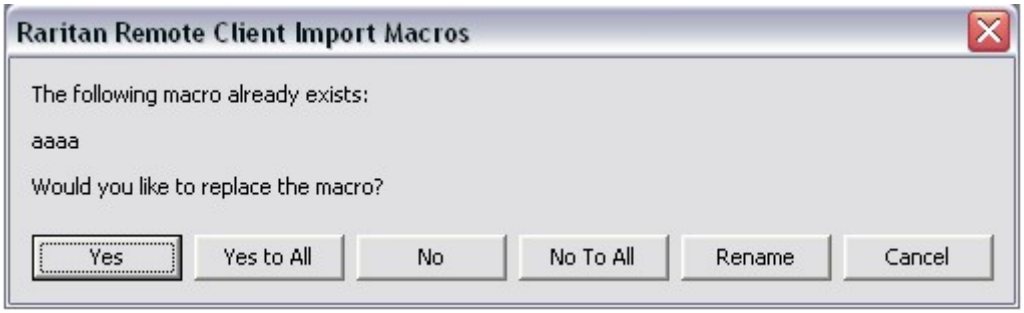
b. If the import fails, an error dialog will open and will display a message regarding why the import failed. Select OK to continue the import without importing the macros that cannot be imported.

3. Select the macros to be imported by checking their corresponding checkbox or using the Select All or Unselect All options.
4. Click OK and the import will begin.

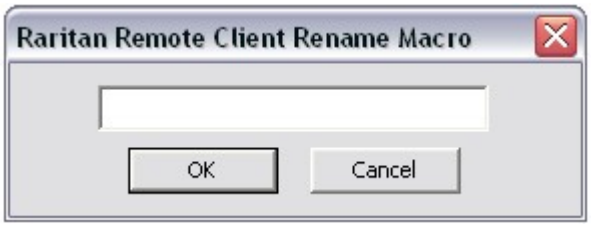


a. If a duplicate macro is found, a dialog will appear. Do one of the following:

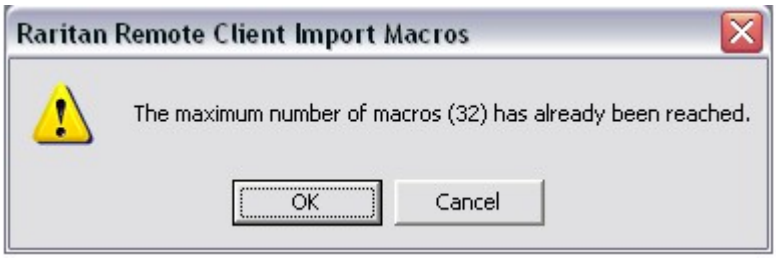
- Click Yes to replace the existing macro with the imported version.
- Click Yes to All to replace the currently selected and any other duplicate macros that are found.
- Click No to keep the original macro and proceed to the next macro
- Click No to All keep the original macro and proceed to the next macro. Any other duplicates that are found will be skipped as well.
- Click Cancel to stop the import.



- Alternatively, click Rename to rename the macro and import it. If Rename is selected, Raritan Remote Client Rename Macro dialog will open. Enter a new name for the macro in the field and click OK. The dialog will close and the process will proceed. If the name that is entered is a duplicate of a macro, an alert will appear and you will be required to enter another name for the macro.



b. If during the import process the number of allowed, imported macros is exceeded, a message will appear. Click OK to attempt to continue importing macros or click Cancel to stop the import process.



The macros will then be imported.

If a macro is imported that contains a hot key that already exists, the hot key for the imported macro will be discarded.

Opening Administrator and Diagnostic Interfaces

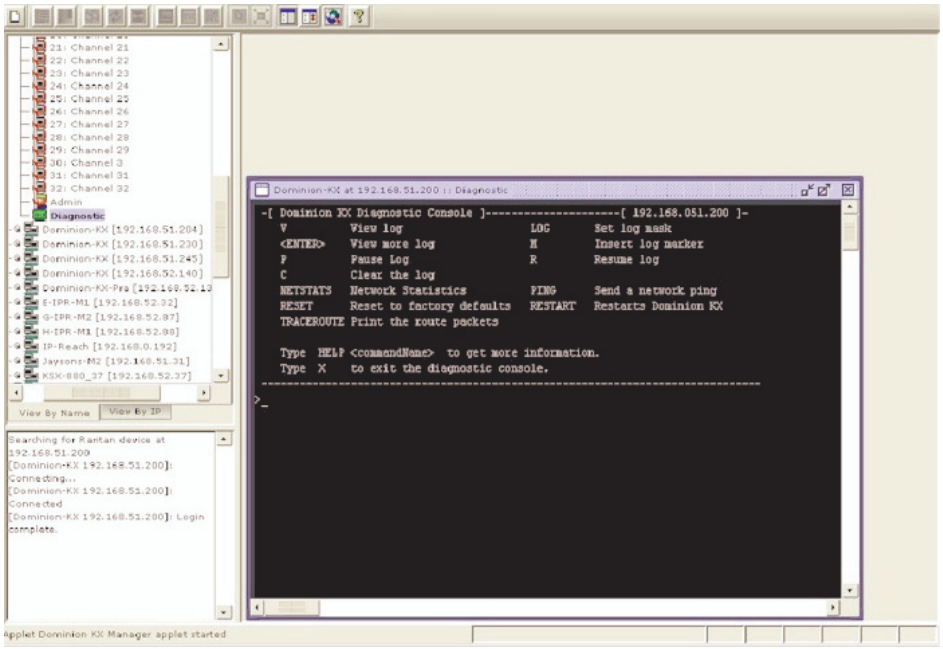
Administrator Interface

For further control of a selected device, in the Navigator, scroll down the list of all the targets associated with the specific device (you may have to expand your view of the device by clicking on the + sign before its name). Next, double-click on the Admin icon at the bottom of the target list. The Administrator login page for the selected device appears.

Refer to the specific Raritan device user guide for additional information and managing the device. The user guide is contained on the CD included with the device shipment or you can download it from the Product Documentation page on Raritan's website: http://www.raritan.com/support/productdocumentation.

Diagnostic Interface (excluding Dominion KX II)

Access the device's diagnostic console by double clicking on the Diagnostic icon at the bottom of the target list in the Navigator. Scroll down the list of all the targets associated with the device (you may have to expand your view of the device) and double-click on the Diagnostic icon at the bottom of the target list.



Special Characters in MPC

The following table identifies the special characters that can be used in MPC:

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

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

Chapter 3 Administrative Functions

In This Chapter

The Dominion KX Manager is used to manage both the Dominion KX and the KX101 product lines. When running on a Dominion KX, features specific to the KX101 are disabled, and when running on a KX101, features specific to the Dominion KX are disabled. Specifics are called out throughout this chapter.

Launching Dominion KX Manager

The Dominion KX Manager is a Java applet, which requires Java to function. When launching Dominion KX Manager via the web, KX Manager checks the client's version of Java. If the version is incorrect or outdated, KX Manager leads you through the updated Java installation.

The Dominion KX Manager currently requires the following Java versions:

- Sun Java 1.4.2_05 or greater
- Sun Java 1.5.0 or greater except Sun Java 1.5.0_02, due to issues with this Java version

Note: Because of a limitation in the JRE, Linux and Solaris clients receive an invalid response from Alt-Gr on UK Language keyboards. Linux and Solaris do not pick up events for the Alt-Gr key combination for Java 1.4.2 or 1.5. Java 1.6 appears to improve on this, although the keyPressed and keyReleased events for Alt-Gr still identify it as an "unknown key code".

Also, a key pressed in combination with Al-tGr (such as on the UK keyboard AltGr-4, which is the Euro symbol, will only generate a keyTyped followed by a keyReleased event for that value, without a keyPressed event. Java 1.6 improves upon this by filling in the keyPressed event as well.

Launch KX Manager in one of these ways:

- Via RRC/MPC by clicking a device's Admin Port.
- Directly from a web browser by entering: http://IP-ADDRESS/admin 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.

- If you are using Internet Explorer (IE), launch your browser and type the following URL: *http://IP-ADDRESS/admin*
- If you are using Netscape version 7.1 or higher, launch your browser and type the following 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.

Important: Regardless of the browser you use, you must allow pop-ups from the Dominion device's IP address in order to launch KX Manager.

1. Username/Password: Log in to KX Manager with an administrator's user name and password (defaults: admin and raritan (all lower case)). To ensure security, change the default user name and password as soon as possible
2. Port: If your device has been configured to use a different TCP port than the default port 5000, type that number here.

Note: Due to a Java issue, before upgrading a device, if you launch KX Manager, upgrade the device, and then re-launch KX Manager, you will either generate a Java Exception or get an older version of KX Manager. To fix this problem, exit all instances of your Browser before upgrading your device.

KX Manager Interface

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

There are three ways to view devices. Click on the View 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

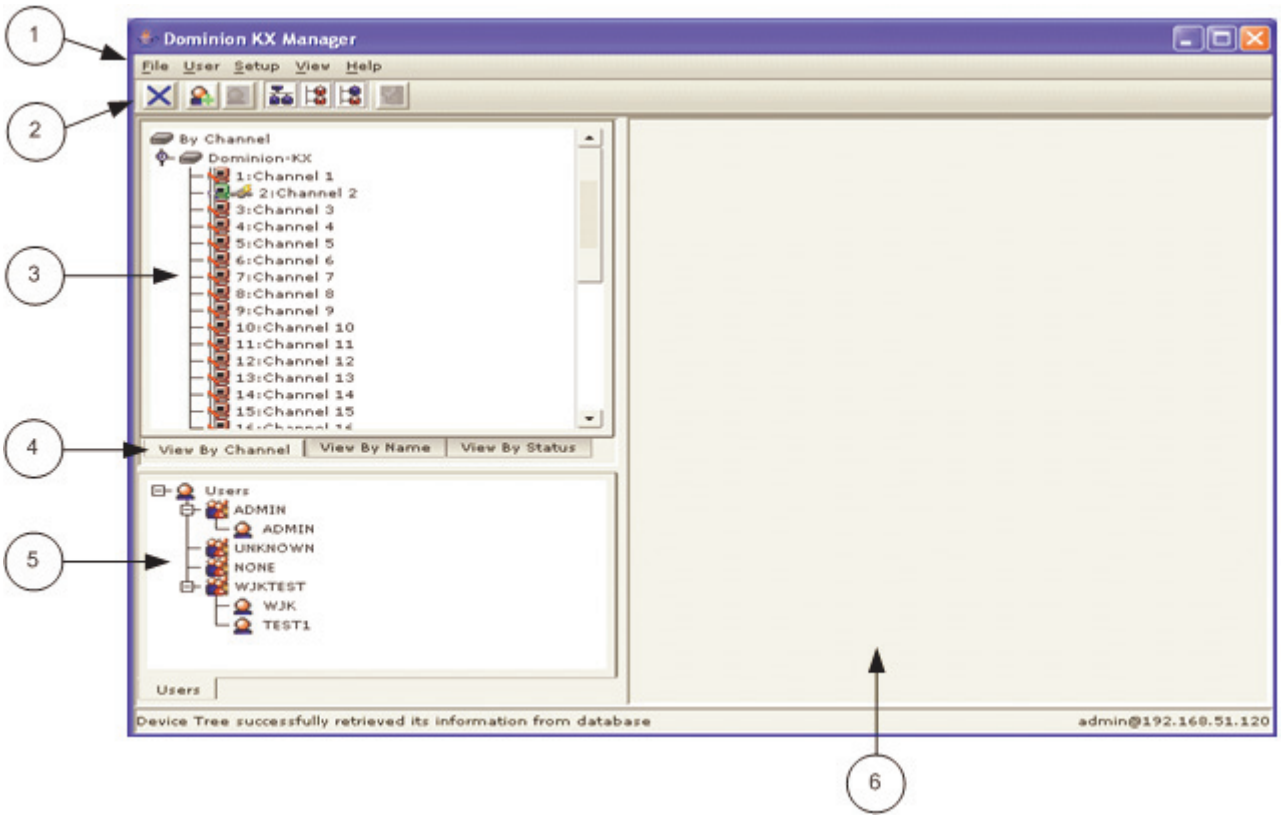


Diagram key	
1	Menu Bar - Holds drop-down command menus for working in KX Manager.
2	Toolbar - Shortcut buttons for the most commonly-used commands in KX Manager.
3	Device Tree - View all devices in your KX configuration .
4	View Tabs - View devices in the Device Tree By Channel, By Name, or By Status.
5	User/Group Tree - View all Users and Groups in your KX configuration.
6	Details Panel - Detailed information on objects selected in the trees appears in this section.

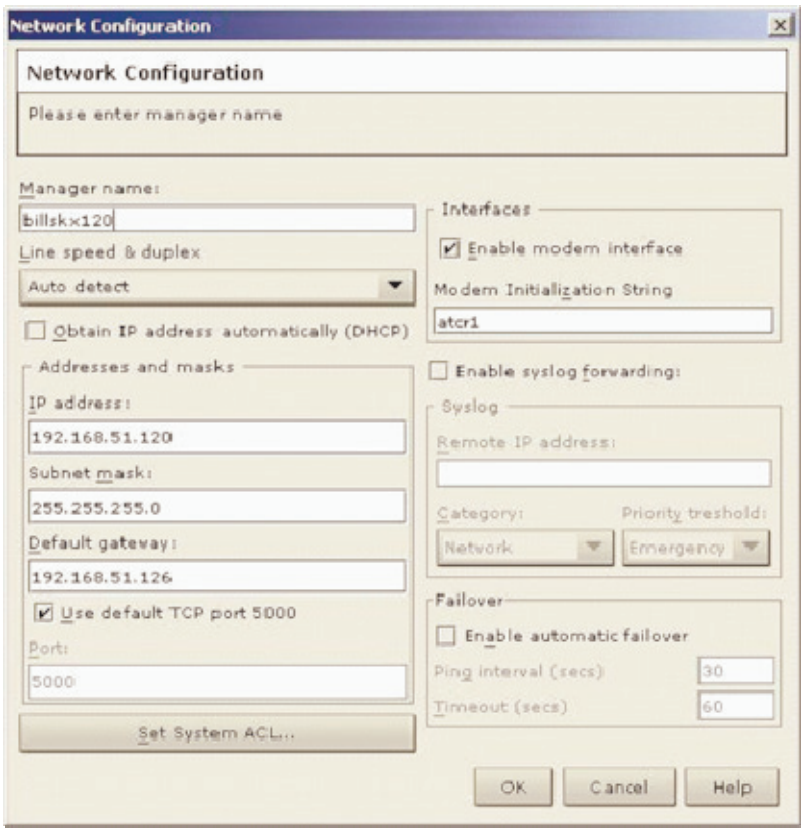
Network Configuration

Use the Setup menu to customize network configuration settings like the IP address and Ethernet speed on your Dominion KX unit. If you have a remote connection to KX Manager, you must reboot the unit after making network configurations in order to activate the new settings. Electing to apply new network settings will log out any users connected through the local console.

Important: Before changing network configuration values, ensure that there are no other active user connections to the device since all connections will be dropped when the KX unit reboots.

➢ ***To configure network settings:***

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



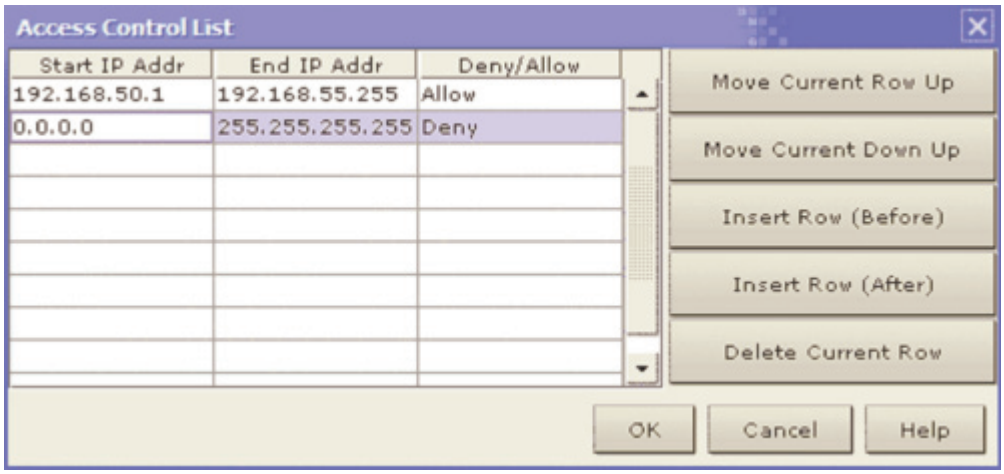
2. Configure the network using the following configuration elements:
   - Manager name: Type a unique name for the device. The default name for a Dominion KX unit is: "Dominion-KX" and for a KX101 unit is KX_KIM-<last five digits of serial number>, for example, a KX101 with serial number S00002 would have a default name of KX_KIM-00002. Remote users will see and use this name to identify this particular device. However, if an MPC or 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.

- Modem Initialization String: Used to configure modem settings. Because different modems have different ways of settings these values, this document does not specify how to set these values, rather the user should refer to the modem to create the appropriate modem-specific string.
  - Modem Settings:
  - Enable RTS/CTS flow control
  - Send data to the computer on receipt of RTS
  - CTS should be configured to only drop if required by flow control.
  - DTR should be configured for Modem resets with DTR toggle.
  - DSR should be configured as always on.
  - DCD should be configured as enabled after a carrier signal is detected. (that is, DCD should only be enabled when modem connection is established with the remote side)
  - If the modem string is left blank, the following string is sent to the modem by default: ATS0=0Q0&D3&C1
- 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.
- Enable syslog forwarding: Click on this checkbox 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.



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 the Dominion KX only from a given IP address range (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.

Important: Note that ACL rules are evaluated in the order in which they are listed. For instance, if in the example, the two ACL rules were reversed, the 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 checkbox to allow the Dominion KX to automatically recover its network connection using a second network port if the active network port fails. Ping interval determines how often the 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. Default Ping interval: 30 seconds; default Timeout: 60 second.

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

3. Click OK to set Network Configurations. If your changes require rebooting the device, a reboot message appears. Reboot the device as required.

Security Settings

1. On the Setup menu, click Security, and then click Setting. The Security Settings window appears.
2. Encryption mode - click on the drop-down arrow to select one of the following:

- No Encryption: Nothing is secure. The communication channel is open to anyone to read and there is no data encryption.
- 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.

3. PC share mode - Determines global concurrent remote access, enabling up to eight remote users to simultaneously log in 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. If there is a remote user and a local user sharing the target, control is based on first active keyboard/mouse input. However, if only remote users are sharing targets, each remote user has equal keyboard and mouse control. PC share timeout value is the idle time that is used to determine when a remote user or local user can take control of the keyboard/mouse from the other. Uneven control will happen if a user does not stop typing or moving the mouse. Automatic color calibration for the session is based on the first connected user's settings; subsequent connected users may notice visual differences from their usual calibration. The first user's settings are the default settings for the duration of the session.

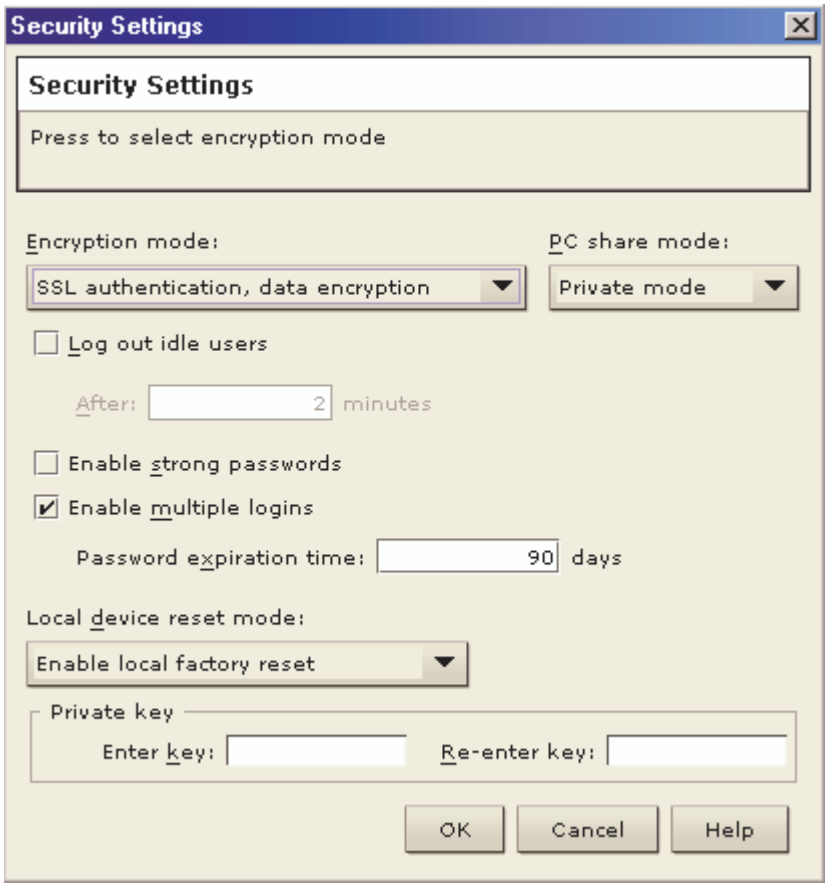
Note: PC share mode is a global setting. For individual user access settings see Keyboard and Mouse Control and Concurrent Access Mode on the User Account Settings page. Each user profile can be set individually to enable/disable keyboard and mouse control, and concurrent access. PC share timeout should remain the default value and should not change before switching to Private mode.

4. Log out idle users: Click on the checkbox 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.

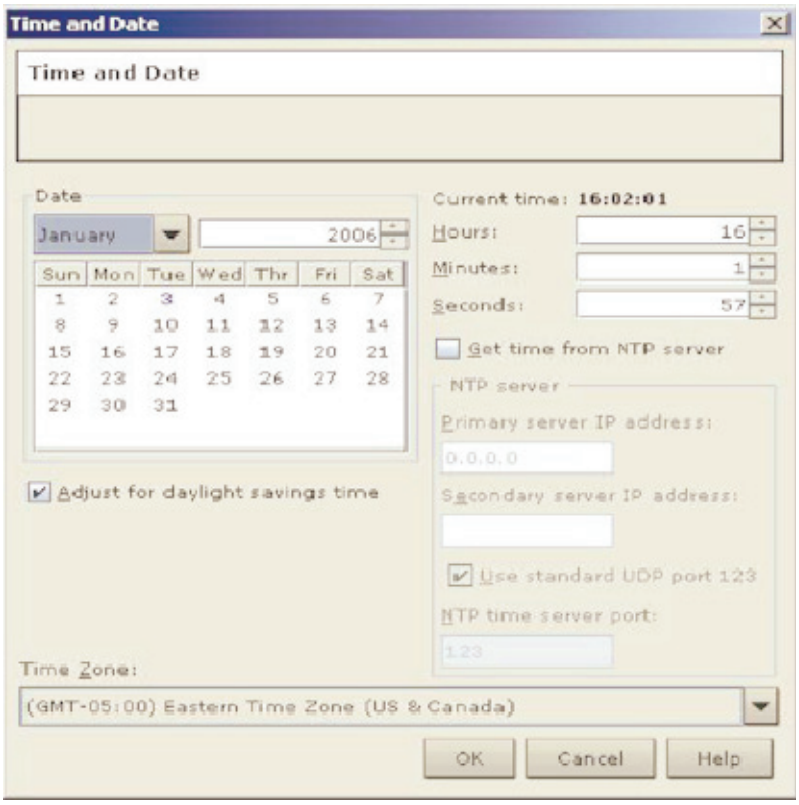
5. Enable strong passwords: Requires user passwords to have a minimum of 6 characters with at least one alphabetical character and one non-alphabetical character (punctuation or number). The first four characters of the password and the user name cannot match. Strong password rules affect only those usernames and passwords stored by the 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 (see the section Remote Authentication in this chapter for more information on remote authentication).
6. Enable multiple logins: When this rule is selected, a given user name/password combination can be connected into the device from multiple client workstations at a time.

7. Password expiration time: Type a number of days in this field to force users to change their passwords after a set duration.
8. 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.
9. Re-enter 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.
10. Local device reset mode: Determines how the local factory and password reset feature in the local console operates (see the Local Console Access chapter for additional information). 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
11. Click OK to set Security Configurations.



Time and Date

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



Users, Groups, and Access Permissions

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 Raritan Customers Upgrading from Previous Firmware Versions

If you previously configured Raritan products 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.

Note to CC-SG Users

If you are using the Dominion KX in a CommandCenter Secure Gateway configuration, this section of the user guide does not apply to you. When the device is controlled by CommandCenter Secure Gateway, CC-SG determines the allowed users and groups. See the CommandCenter Secure Gateway User Guide, Administrator Guide, or Deployment Guide on the Raritan website (*www.raritan.com* http://www.raritan.com).

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 page displays both User and Group names created for the device. Users belonging to a Group are nested under their group name.

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

Group name	Description
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, and a login attempt is successful but no user group is returned by the remote authentication server.

Group name	Description
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 the Dominion KX.

An individual group is essentially a "group" of one. That is, the specific user is in its own group, not affiliated with other real groups. Individual groups can be identified by the "@" in the Group Name. The individual group allows a user account to have the same rights as a group.

Creating or Editing 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).

➢ ***To create a new user group:***

1. On the User menu, click Add User Group. The Add Group dialog appears.
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.
   - The first group of permissions (the upper table) controls user authorization for using these specific administrative functions within KX Manager and RRC. For example, if you check the box before Manage user accounts, the members in this group can create new user accounts in KX Manager. Likewise if you check Restart, shutdown device, the members can reboot the Dominion KX from RRC. Note that in order to access the diagnostic panel in RaritanConsole, both Manage diagnostics and Path, time/date... must be checked. Several administration functions are available within MPC and from the Dominion KX's Local Console; these functions are available only to members of the default ADMIN group. If you enable Manage user accounts and Manage user groups, a confirmation windows appears to allow you to confirm your choice. Click OK to confirm.

- 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 the Dominion KX with concurrent view and control of targets, such as a PC Share session. (Modem access is disabled in KX101.)

4. In the Basis panel of the page, 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. Click on one of them to apply that group's properties to the group you are adding.

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

---

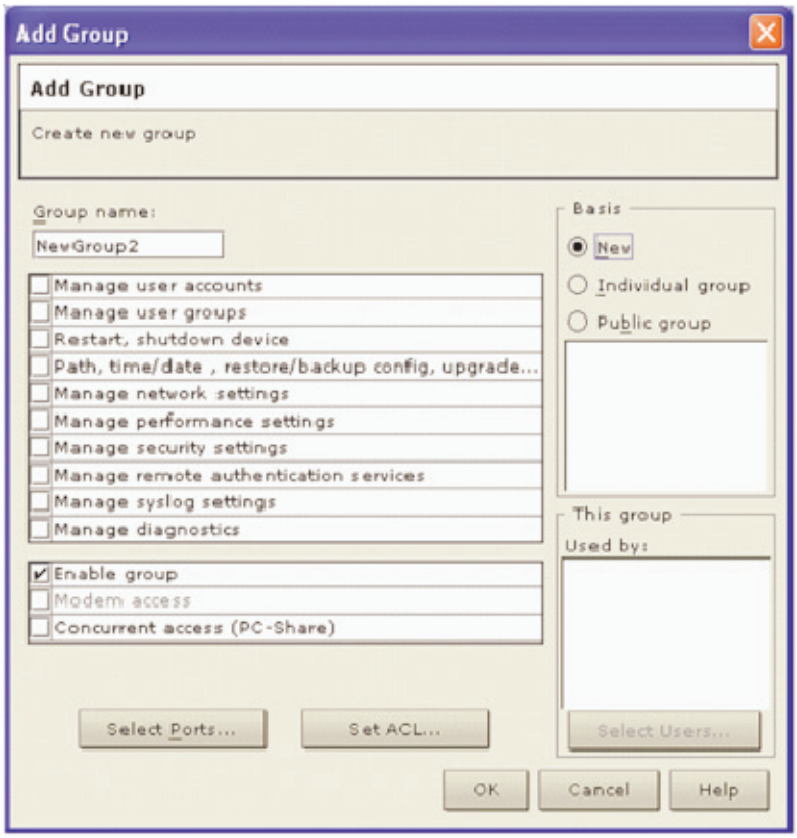
5. Other permission elements on the Add Group or Edit Group screens include:

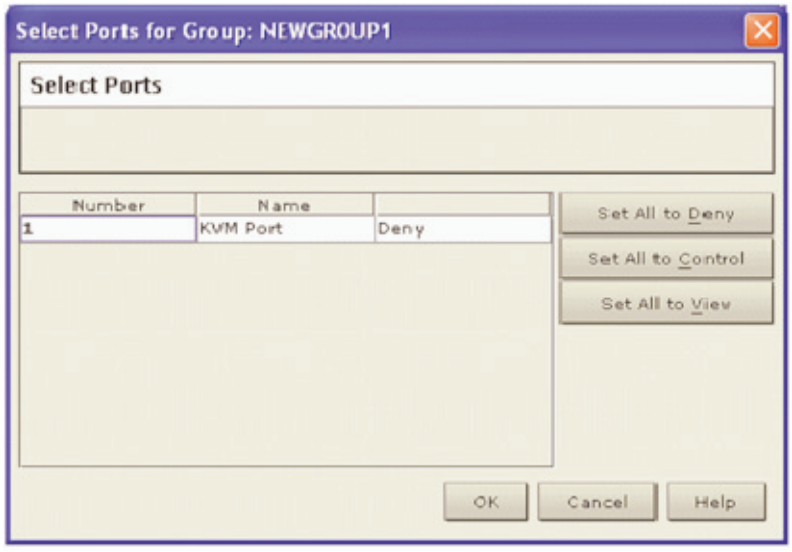
   - This Group panel, Used by field - Displays all users assigned to this group. The Select Users button allows administrators to move previously configured users into this group.
   - Select Ports - Click this button to specify which server ports can be accessed by users who belong to this group. For 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.
   - 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).

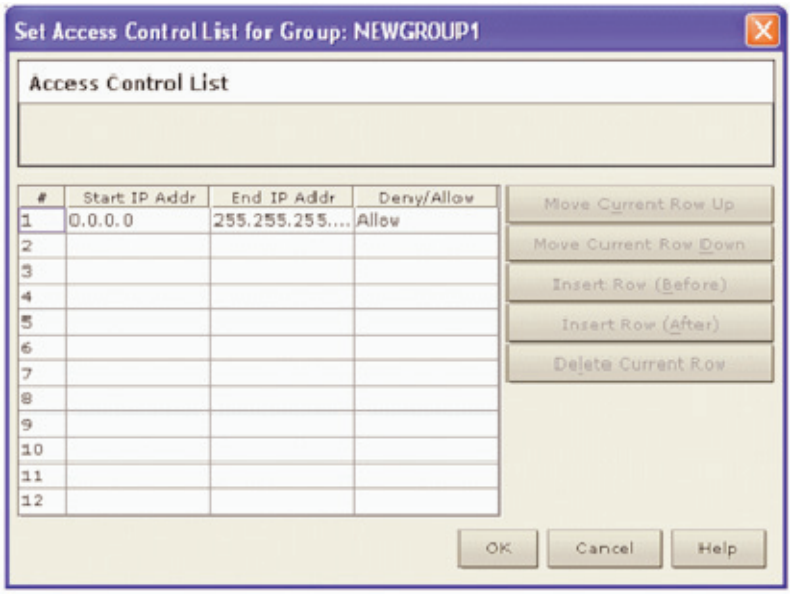
Important: Note that ACL rules are evaluated in the order that they are listed

---

6. Click OK to save Group properties.



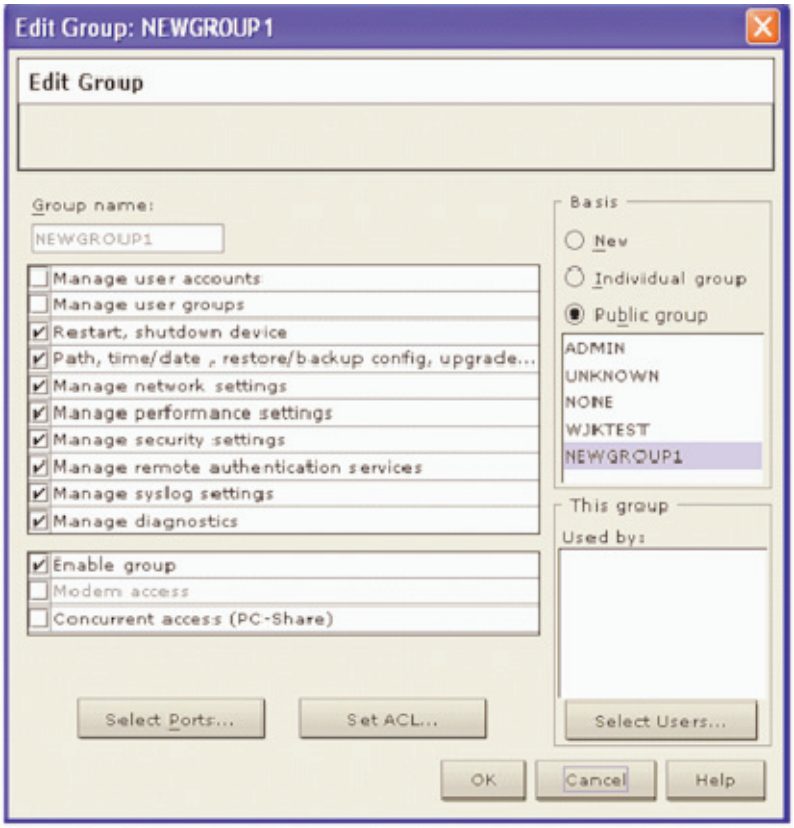




➢ ***To edit an existing User Group:***

1. Select the group that you wish to edit in the user list, right-click on the icon, and select Edit User Group. The Edit Group dialog appears.
2. Edit the information as needed.

3. Click OK to save Group properties.



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. Alternatively, click [Select Users] in the Groups dialog.

When the Select Users dialog appears, add users to the group by selecting the user in the All Users list and clicking the Add button. This will move the user to the Users in Group list.

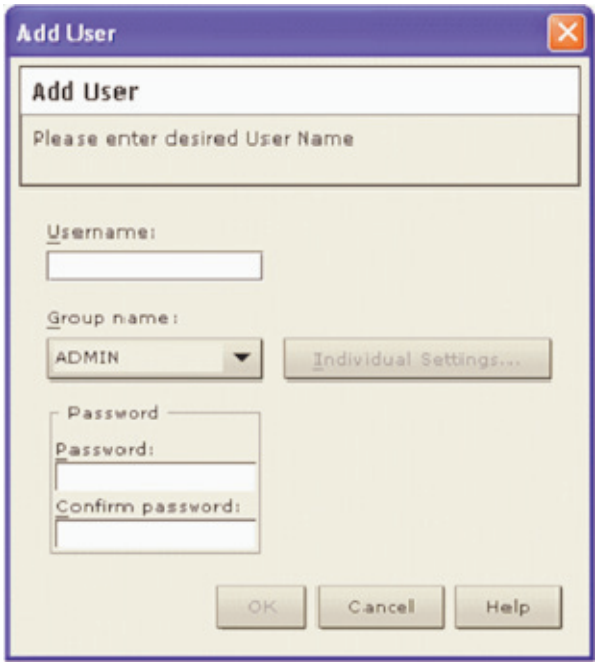
Deleting User Groups

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.

Creating or Editing Users

➢ ***To create a new user:***

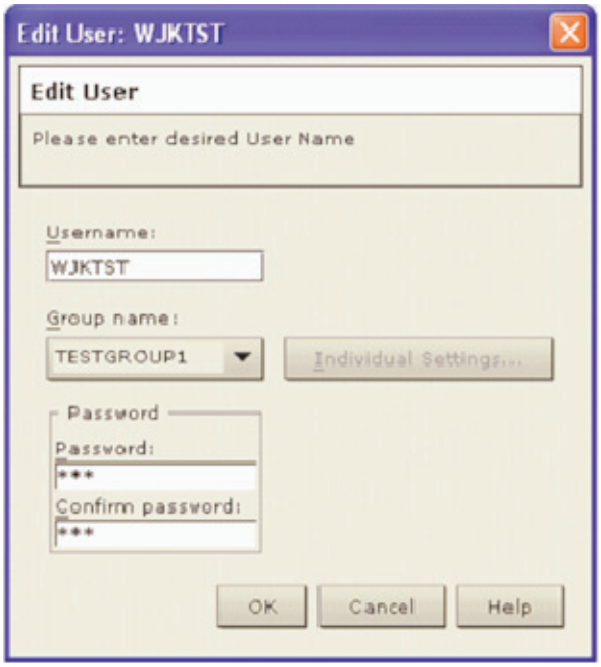
1. On the User menu, choose Add User. The Add User dialog appears.
2. Type a unique user name in the Username field.
3. Click on the Group Name drop-down arrow and select a User Group to which you want to assign this user. If you do not want to associate this user with an existing User Group, select 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 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.



➢ ***To edit an existing user:***

1. In the user list, select the user that you wish to edit, right-click on the icon, and select User Properties. The Edit User dialog appears.
2. Edit the fields as needed.

3. Click OK to save user properties.



Deleting 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

Note to Raritan Customers Upgrading from Previous Firmware Versions

If you have previously implemented RADIUS authentication on Raritan products running legacy firmware versions earlier than v3.2, read this entire section carefully.

Beginning with firmware version v3.2 and later, the implementation of external authentication has changed significantly to provide more flexible and powerful configurations.

Note to CC-SG Users

If you are using the Dominion KX in a CommandCenter Secure Gateway configuration, this section of the user guide does not apply to you. When the device is controlled by CommandCenter Secure Gateway, CC-SG determines Remote Authentication. See the CommandCenter Secure Gateway User Guide, Administrator Guide, or Deployment Guide on the Raritan website (***www.raritan.com*** http://www.raritan.com).

Supported Protocols

In order to simplify management of usernames and passwords, the Dominion KX provides you with the ability 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 the Dominion KX. If it has the IAS (Internet Authorization Server) component, a Microsoft Active Directory server can also serve as a RADIUS authentication source.

Note on Remote Login Usernames and Passwords

The Dominion KX login user name and password are both limited to 16 characters. Keep this limitation in mind when setting up remote authentication, because remote authentication usernames and password could exceed this minimum length.

Remote Authentication Implementation

Priority

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

Username status	Action
If the user name is not found in the Dominion KX internal database	Request is forwarded to external authentication server to determine whether the login is allowed or denied.
If the user name is found in the Dominion KX internal database and password is correct	Login is allowed.
If the user name is not found in the Dominion KX internal database and password is incorrect	Login is denied; the request *does not* get forwarded to the external authentication server.

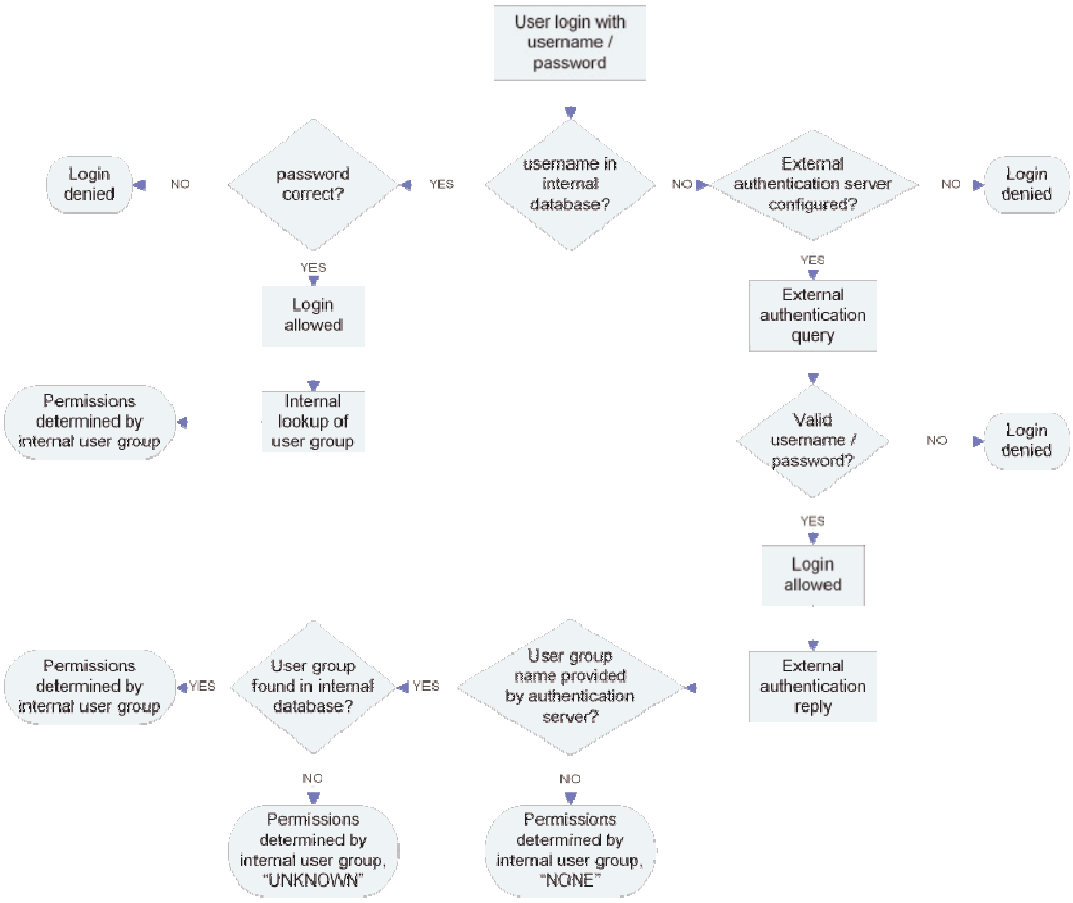
Authentication vs. Authorization

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.

The flow diagram illustrates the steps taken:

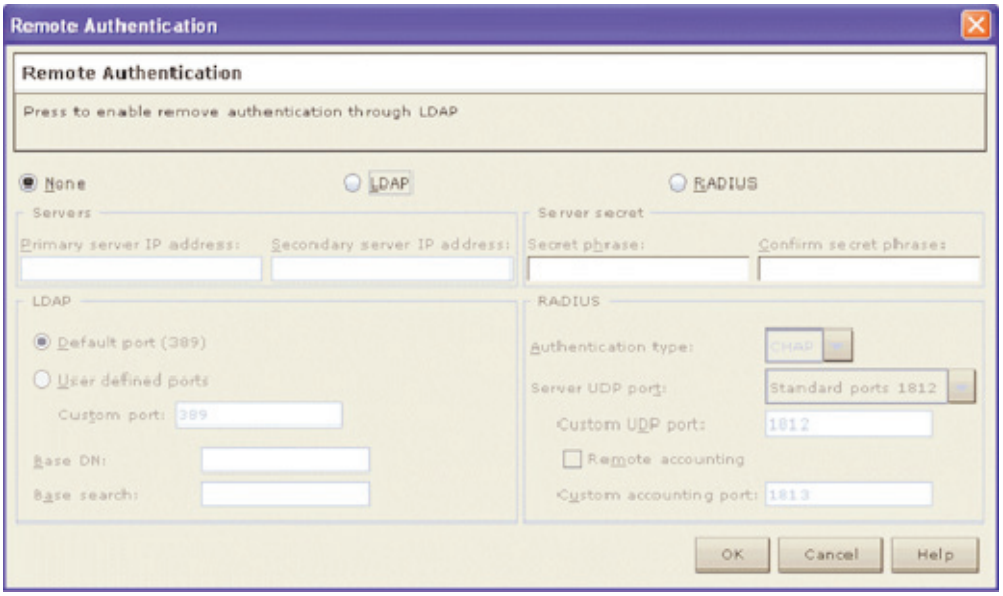


Note the importance of the group to which a given user belongs, as well as the need to configure the groups named, “UNKNOWN” and “NONE.” If the external authentication server returns a group name that is not recognized by the KX101, that user's permissions are determined by the permanent group named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

See the sections LDAP or RADIUS 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, choose Security, and then choose Remote Authentication to configure your Dominion unit for remote authentication. The Remote Authentication dialog appears:



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, 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, 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.

Note: Upon receipt of an Access-Request from a valid client, an appropriate reply MUST be transmitted. An Access-Request SHOULD contain a User-Name attribute. It MUST contain either a NAS-IP-Address attribute or a NAS-Identifier attribute (or both). Raritan recommends using the NAS-IP-Address matches <IP Address>.

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:

- Default Port/User Defined Port: By default, LDAP uses port 389. To use a different port, click User defined ports, and then enter a different port number in the Custom port field.
- 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 the Dominion KX.

Returning User Group Information via LDAP

When an LDAP authentication attempt succeeds, the Dominion KX 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. Consult your authentication server administrator to enable this attribute.

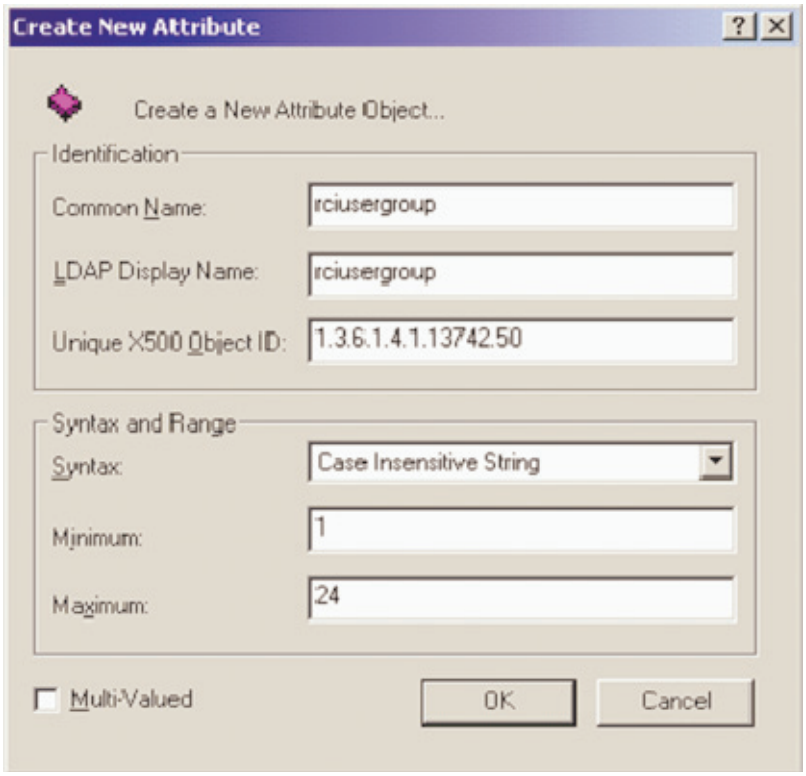
Returning User Group Information from Microsoft Active Directory

1. 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. Refer to your Microsoft documentation for more detail.
2. Install the schema plug-in for Active Directory - refer to Microsoft Active Directory documentation for instructions.
3. Run Active Directory Console and select Active Directory Schema.
4. Setting the Registry to Permit Write Operations to the Schema
5. To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.
6. Right-click the Active Directory Schema root node in the left pane of the window, and then click Operations Master.
7. Click on the checkbox before The Schema may be modified on this Domain Controller.
8. Click OK.

➢ ***To create a new attribute:***

1. To create new attributes for the rciusergroup class:
2. Click the + symbol before Active Directory Schema in the left pane of the window.
3. Right-click Attributes in the left pane.

4. Click New, and then select Attribute. When the warning message appears, click Continue and the Create New Attribute window appears.

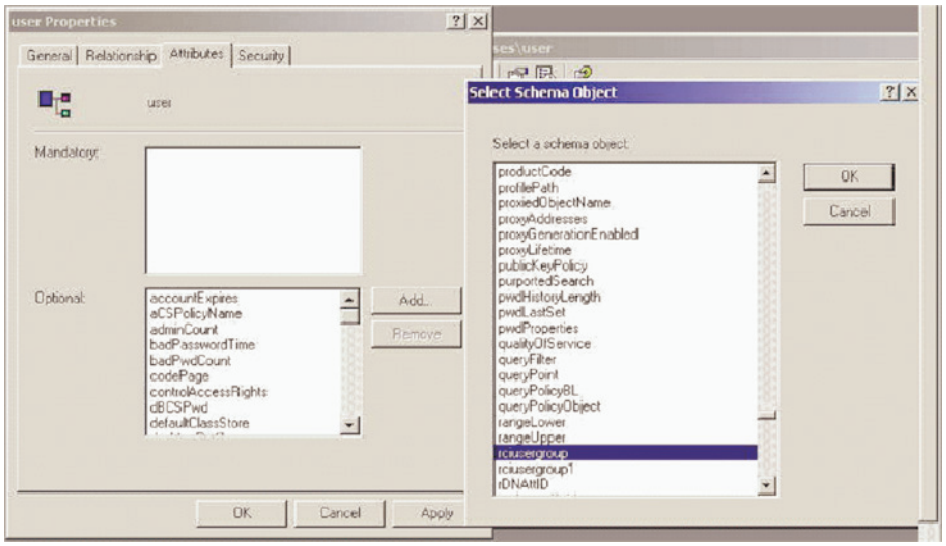


5. Type rciusergroup in the Common Name field.
6. Type rciusergroup in the LDAP Display Name field.
7. Type 1.3.6.1.4.1.13742.50 in the Unique x5000 Object ID field.
8. Click on the Syntax drop-down arrow and select Case Insensitive String from the list.
9. Type 1 in the Minimum field.
10. Type 24 in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

➢ *To add attributes to the class:*

1. Click Classes in the left pane of the window.
2. Scroll to the user class in the right pane, and right-click on it.
3. 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.



7. Click OK.
8. Click OK.

➢ ***To update the schema cache:***

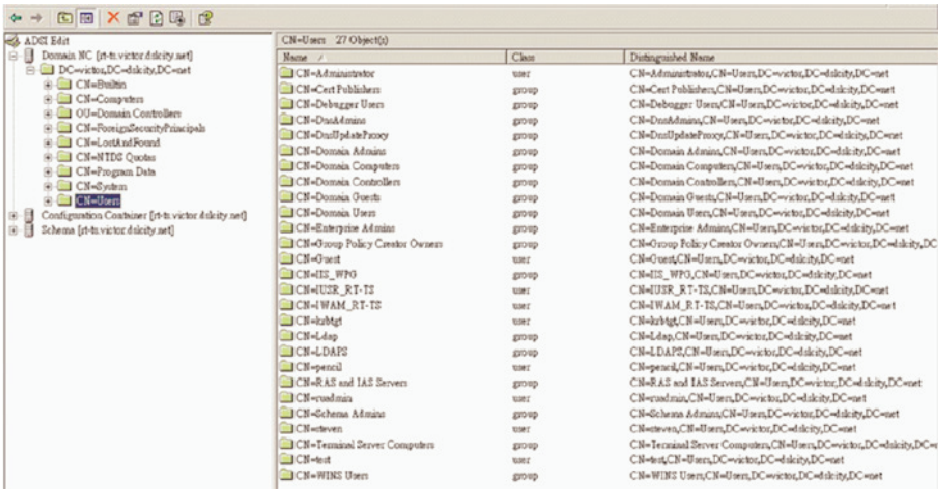
1. Right-click Active Directory Schema in the left pane of the window and select Reload the Schema from the shortcut menu.
2. Minimize the Active Directory Schema MMC console.

Editing RCI User Group Attributes for User Members

To run Active Directory script on Windows 2003 server, 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.mspx
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/ebca3324-5427-471a-bc19-9aa1decd3d40.mspx.

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

1. On the Windows Start menu, choose Run.
2. Type regsvr adsiedit.msc. The ADSI Edit dialog appears.



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

9. Click OK.

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

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

Attribute	Data
USER-NAME	The user name entered at the login dialog.
USER-PASSWORD	In PAP mode, the encrypted password entered at the login dialog.
CHAP-PASSWORD	In CHAP mode, the CHAP protocol response computed from the password and the CHAP challenge data.
NAS-IP-ADDRESS	The 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.

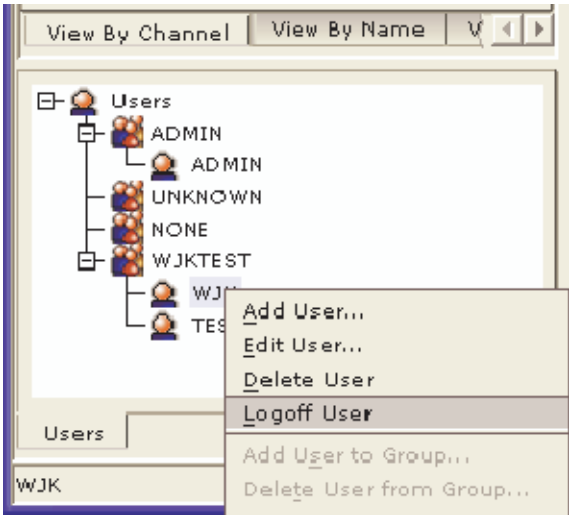
The KX unit sends the following RADIUS attributes to the RADIUS server with each accounting request:

Attribute	Data
SESSION-TYPE	Either START (1) for log in or STOP (2) for log out.

Attribute	Data
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	The user name entered at the login dialog.
NAS-IP-ADDRESS	The 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.
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 the 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

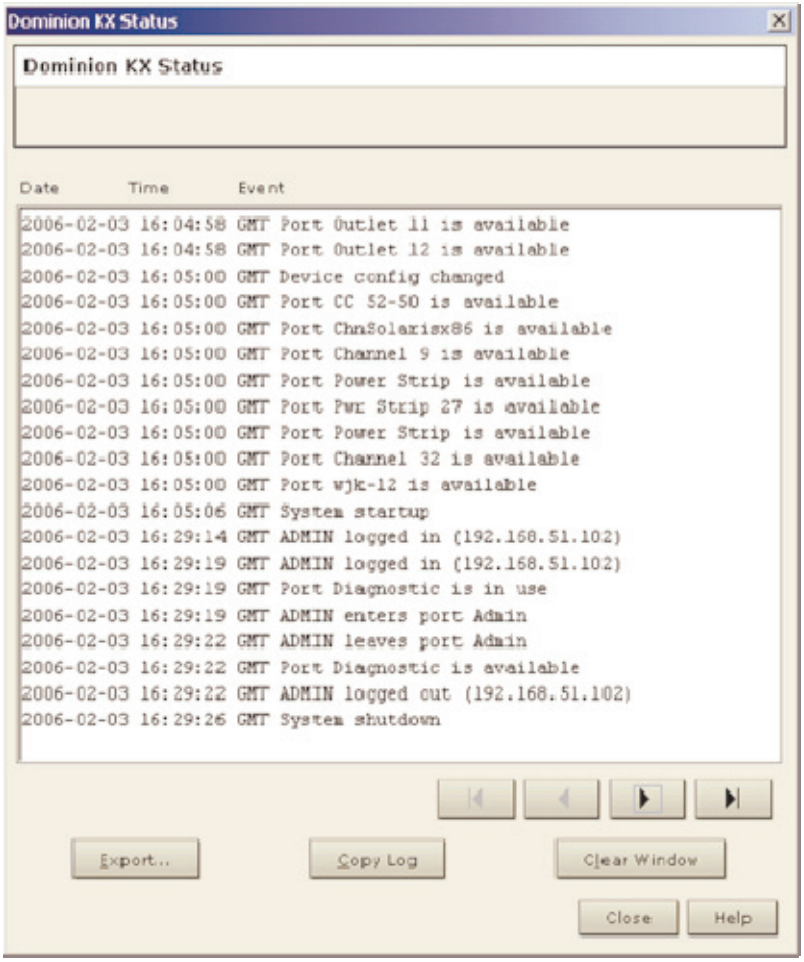
To manually log a user off a device, select that user in the Navigator, right-click on the user icon, and select Logoff User.



Viewing KX Unit Event Log (Status)

1. On the Setup menu, choose Status to view the device's Event Log. The Status dialog appears and displays events by date and time.
2. Click Export and browse for a location to save the displayed log file to a text file.

3. Click Copy Log to copy the contents to your clipboard.



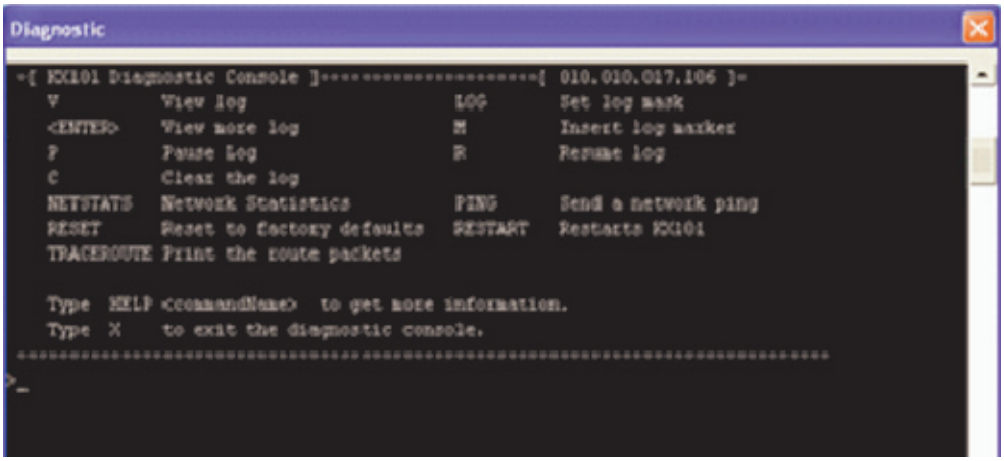
Restarting the Device

To reboot the device, do either of the following:

- Open the RRC/MPC Tools menu and select Restart device. See *Restarting a Device* (on page 127) for more information.
- Right-click the KVM device and select Restart device.

Device Diagnostic Console in KX Manager

1. On the Setup menu, choose Diagnostics to view a Diagnostic window from KX Manager.

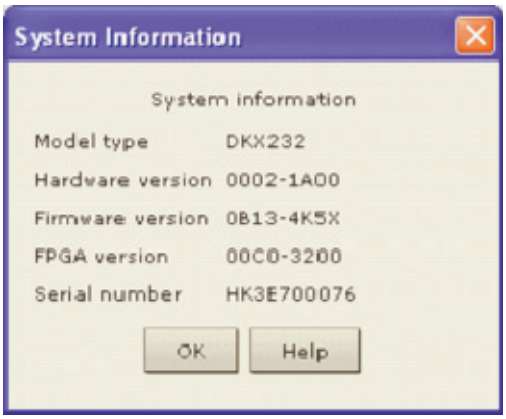


To determine the Firmware Upgrade on the KX device, type *buildinfo* at the prompt and press Enter. For releases KX 1.3 and higher, the Firmware Upgrade Version appears. This version number is in the same format as used on the firmware upgrade page on Raritan's website.

See ***Diagnostic Interface*** (see "Diagnostic Interface (excluding Dominion KX II)" on page 144) for information on performing a device diagnostic in MPC and RRC.

Device System Information

- On the Setup menu, choose System information to view Model type, hardware version, Firmware version, Serial number, and, if applicable, the MAC Address of the device. The FPGA version field is inactive.



Configuration Backup and Restore

➢ ***To backup a device:***

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

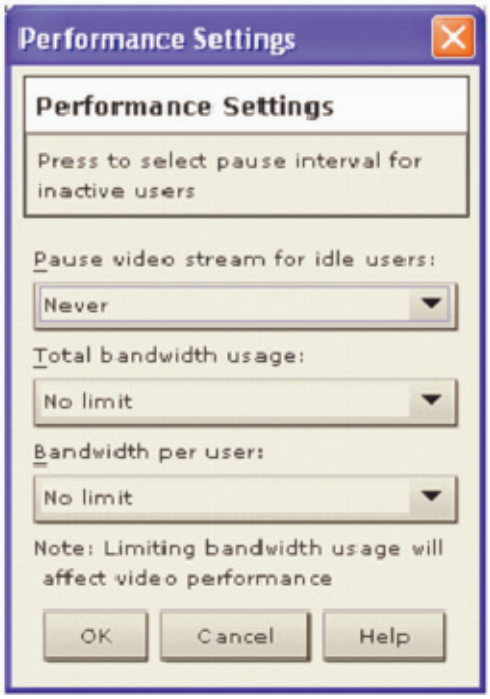
➢ ***To restore a device:***

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

Performance Settings

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

1. On the Setup menu, choose Configuration and then choose Performance. The Performance Settings dialog appears.



- 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, and 120 minutes.

  Note, if Pause Video Stream is enabled and the keyboard or mouse do not respond on the channel after the timeout, disconnect and reconnect to the channel to resume operation.

- 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 and 128Kbps.

- 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, and 128Kbps.

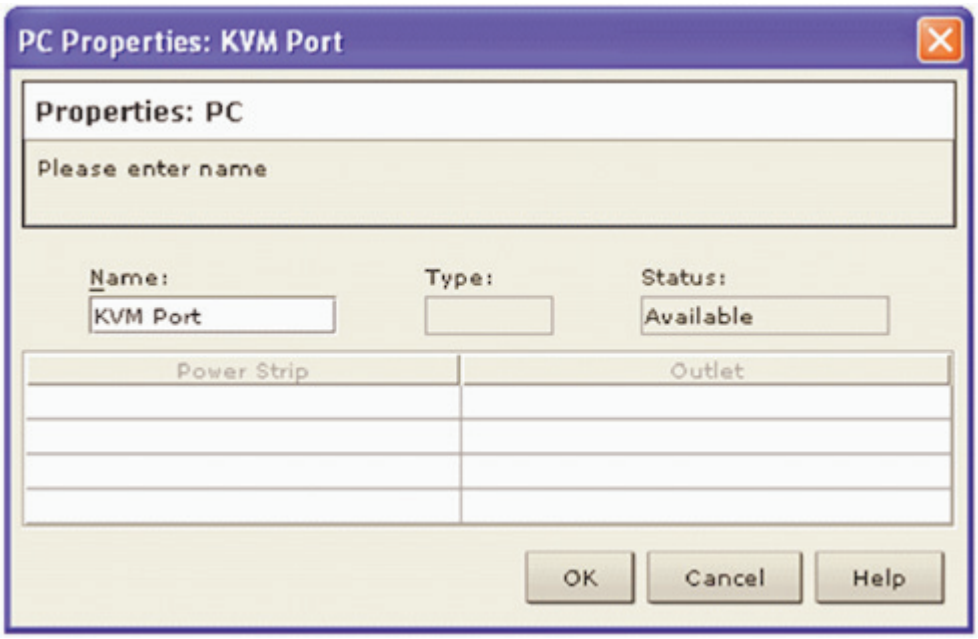
2. Click OK to set Performance Settings.

PC Properties

➢ ***To view PC properties:***

1. Select a server in the server list.
2. On the Setup menu, choose Properties and then choose PC (or select a server in the server list by right-clicking on it and clicking 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 (see the ***Power Control section*** (see "Power Control (Dominion KX only)" on page 185) for additional information).



Power Control (Dominion KX only)

The Dominion KX supports up to eight (8) power strips. Users may group or assign up to four outlets to any of the Dominion channels. Once assigned, the power management function is available in MPC and RRC.

Setup Preparation

You must have a power strip and the P2CIM-PWR Computer Interface Module (CIM). By default the P2CIM-PWR is *not* included with Raritan power strips.

To receive the P2CIM-PWR CIM with the power strip, you must order the power strip with a part number that ends in PK (for example, PCR8-15-PK). Alternatively, the CIM can be ordered separately from the power strip. Raritan devices must be ordered from Raritan or an authorized Raritan reseller.

Connecting the Power Strip

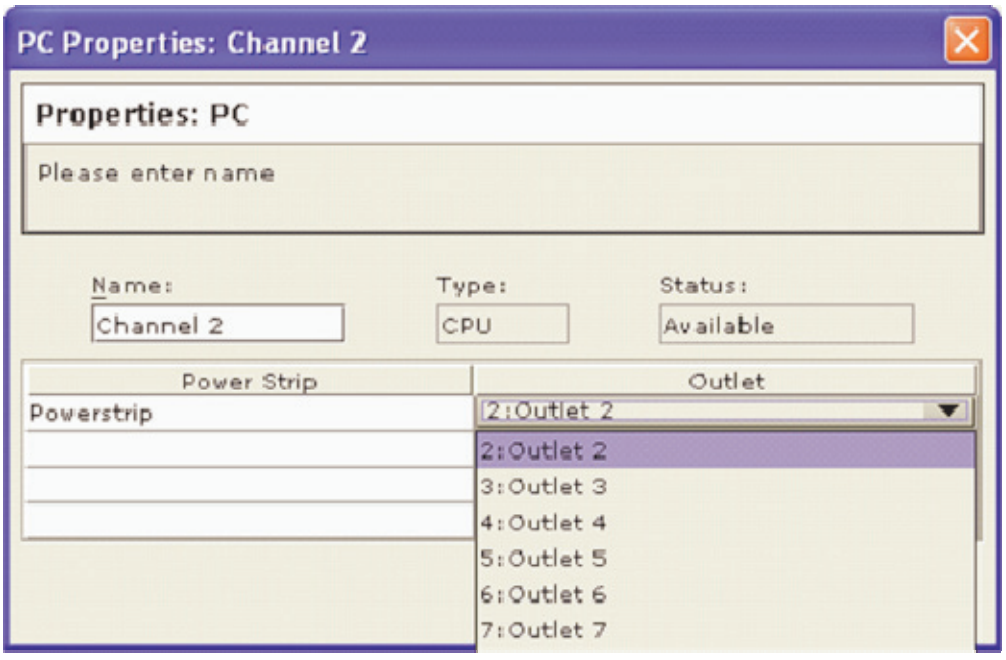
1. Connect the male RJ-45 of the P2CIM-PWR to the female RJ-45 connector on the power strip.

2. Connect the female RJ-45 connector of the P2CIM-PWR to any of the available female system port connectors on the Dominion KX using a straight through Cat 5 cable.
3. Power on the power strip.
4. Power on the Dominion KX unit.

Configuring the Power Strip

Once the power strip has been added, KX Manager will automatically recognize that it is connected. The Device Tree in the left panel of the window will change the appropriate target icon to indicate that a power strip is connected to that port.

1. Select the power strip icon, right-click on it, and then click Properties. When the Power Strip Properties dialog appears, type a name for the new power strip and click OK.
2. In the Devices Tree, select the target server(s) powered through the power strip. Right-click on the server icon and click Properties. The PC Properties window appears.



3. Click on one of the Power Strip rows in the table and a list of available power strips connected to the Dominion KX appears. Click on the appropriate power strip.
4. Click on the Outlet drop-down that is associated the the selected power strip. A list of available outlets is displayed. Select the outlet to which the device is connected.

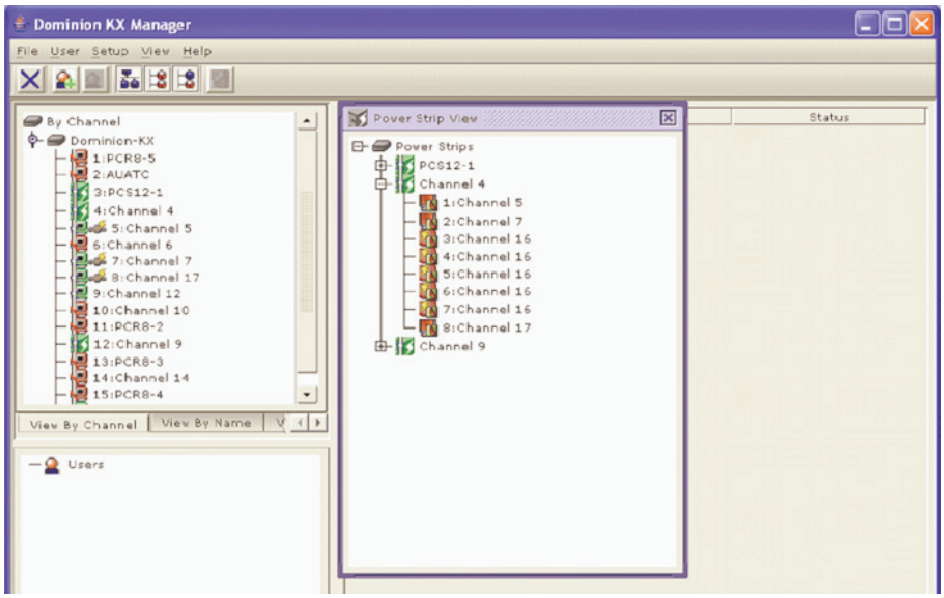
Repeat these steps for all devices plugged into multiple outlets. Once outlets have been assigned, Remote Power Management to the associated server will be available in the associated client software (see *Multi-Platform Client and Raritan Remote Client* (on page 26)).

Note: Be sure to assign the correct outlets to each channel. If more than one outlet is physically associated with a different server, you could accidentally switch the wrong server off.

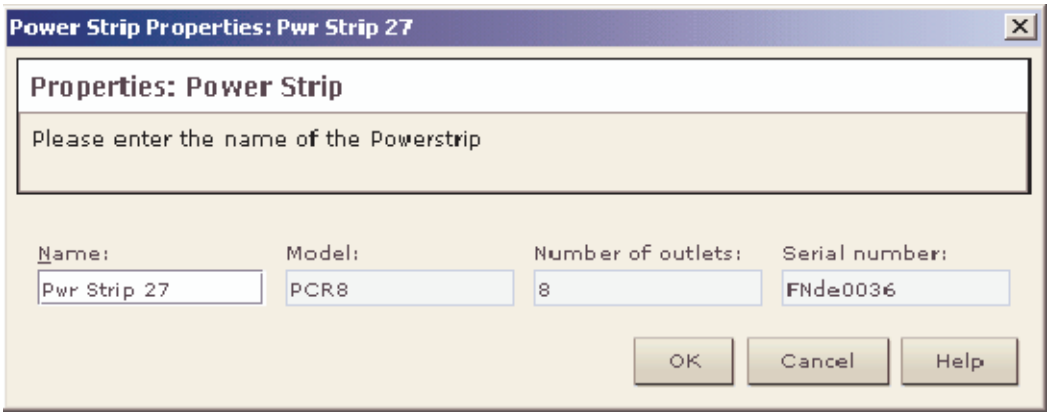
Power Strip Management

➢ ***To view Power Strip Properties, do one of the following:***

- Right-click on the Power Strip channel/icon in the Navigator.
- On the View menu, choose Power Strip. Select a Power Strip in the list, right-click on it, and then click Properties.



The properties listed are name, model, number of outlets, and serial number.



In this dialog, you can change the outlet's name (this is the name that will be displayed in the Power Strip View window), view the device type that is plugged into that outlet (either an associated Paragon Target or a non-associated device), o delete any previously made associations.

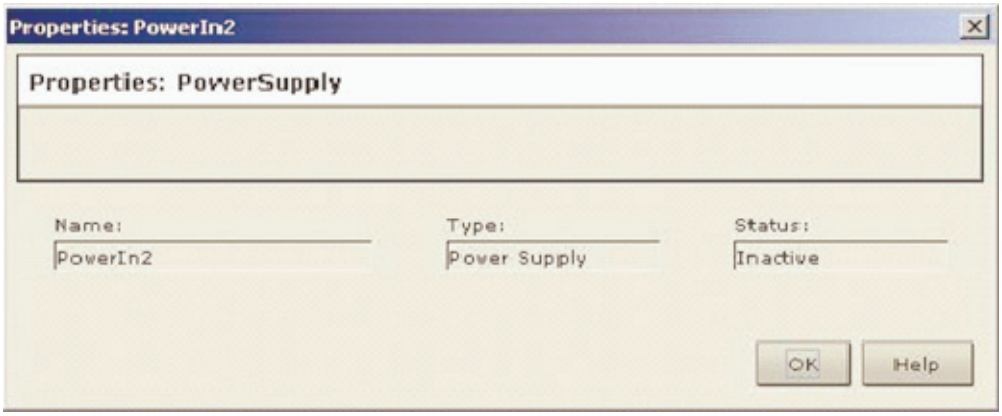
Power Supply Management (Dominion KX only)

The Dominion KX displays the status of its Power Supplies, one per unit, except for the KK464, which displays two Power Supplies. The Power Supply icon in the Navigator indicates whether the Power Supply is Active or Inactive.

	Active Power Supply
	Inactive Power Supply

Power Supply Properties

The Power Supply Properties dialog displays the power supplies status. None of the fields in this window can be edited, as these properties are obtained directly from the Power Supply device.



CC UnManager

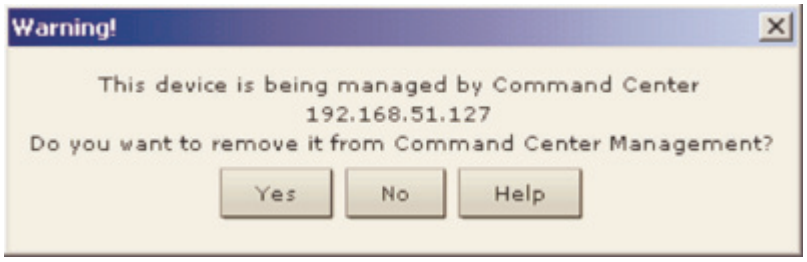
KX Manager supports CC UnManager, an "un-manage" feature. This feature provides you with the ability to remove (un-manage) a device that is managed by Command Center Secure Gateway (CC-SG), but which is not under control by that CC-SG device from CC-SG management. CC UnManager is designed to restore full control to the Dominion unit in the event the CC-SG goes off-line.

If the CC-SG loses communication with the Dominion unit, after 10 minutes the Dominion unit automatically allows users to log in using the Dominion's own internal user and password information.

If users attempt to log in to the Dominion unit while it is under CC-SG control, the Dominion unit will issue either a Communication Error or a Login Incorrect message.

Logging in with CC UnManager

When you launch KX Manager while the Dominion is under CC-SG control, it generates a warning that prompts you to remove it from CC-SG management.



- If you click Yes to remove the Dominion from CC-SG control, KX Manager issues a confirmation window. Click Confirm to remove the Dominion from CC-SG control.

- If you click No and leave the Dominion device under CC-SG management, KX Manager issues a warning that indicates that any changes you make to this Dominion device while it is still under CC-SG management may have negative effects on the CC-SG unit controlling it and on itself.

Activating CC UnManager

If you are already logged in to a Dominion unit that is under CC-SG management, but not under CC-SG control, you can issue the CC UnManager command to remove the Dominion from CC-SG management.

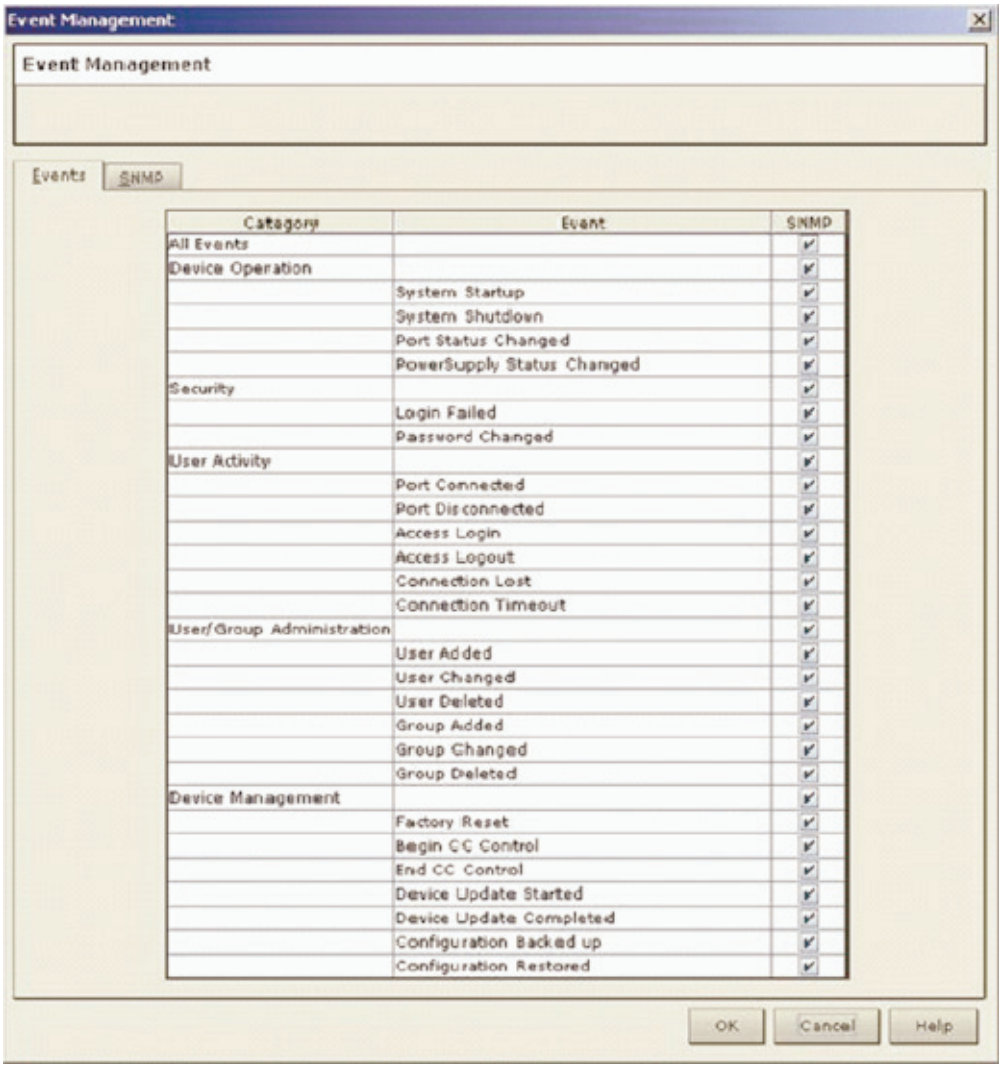
- On the Setup menu, choose Configuration and then choose CC UnManager.

Event Management

The Dominion KX offers SNMP agent support through the Dominion KX's Event Management feature.

1. To run SNMP agent support properly, set the path, time and date permissions.

2. On the Setup menu, choose Configuration and then choose Events. The Event Management dialog appears.



3. Click on the Event Management tab to select and configure events that you want to generate SNMP notification events (traps).
4. Click on the checkboxes associated with the event line items you wish to enable or disable. Enable or disable entire categories by checking or unchecking the specific category line checkboxes. See the SNMP Trap table in the ***SNMP Agent Configuration*** (on page 193) section for additional information on SNMP agents and traps.
5. To configure the Dominion unit as an SNMP agent, click on the SNMP tab. Otherwise, click OK when finished.

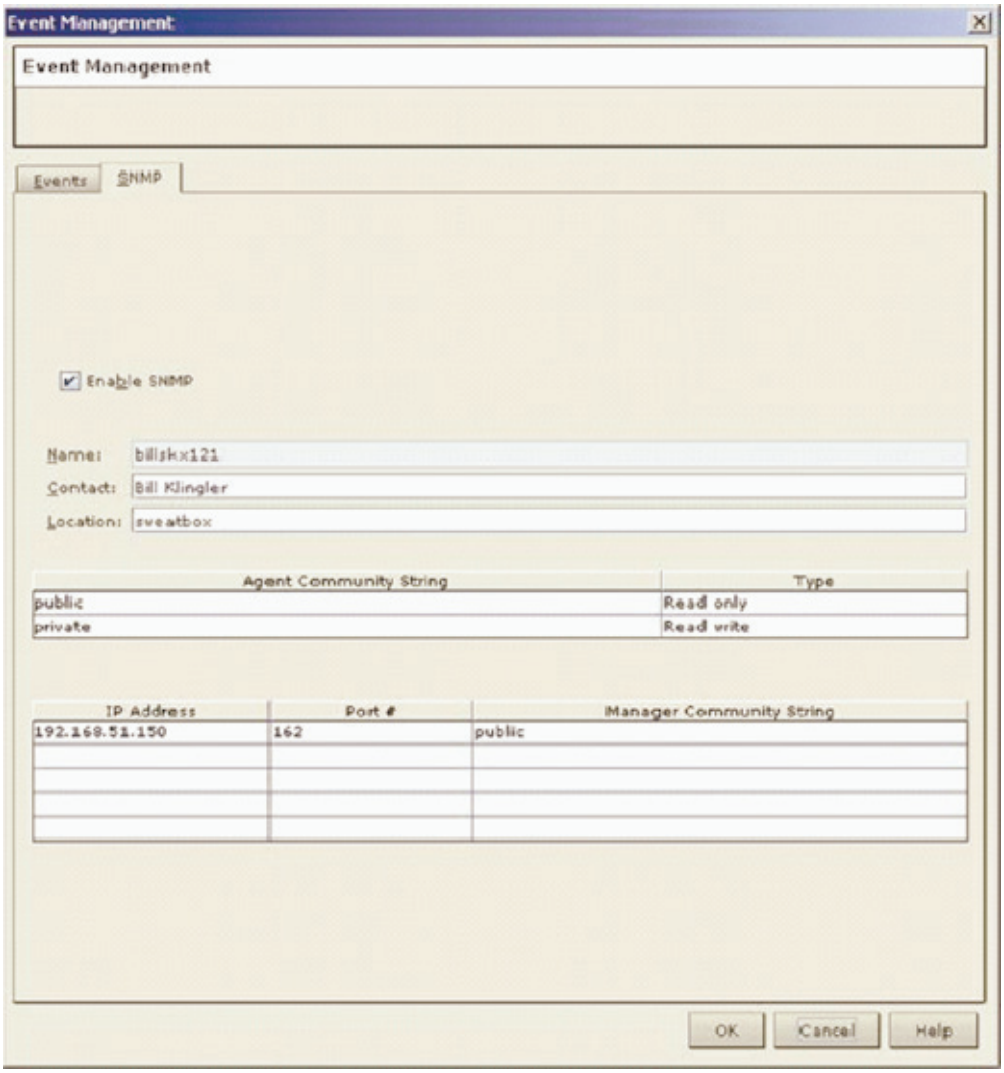
Note: No SNMP traps are generated for the Port Connect and Port Disconnect trap when a user connects or disconnects a Dominion KX device from the local (OSD) port.

SNMP Agent Configuration

Use the SNMP dialog to configure the SNMP connection between the Dominion KX (SNMP Agent) and an SNMP manager.

1. In the Event Management window, click on the SNMP tab.
2. Click on the Enable SNMP checkbox to enable the SNMP Agent feature; uncheck this checkbox to disable SNMP Agent.
3. In the Name, Contact, and Location fields, type the SNMP Agent's (this Dominion unit's) name as it appears in the Navigator panel, a contact name related to this unit, and where the Dominion unit is physically located.
4. Type the Agent's Community Strings (the Dominion unit's strings) and specify whether they are Read Only or Read/Write.
5. Configure up to five SNMP managers with by specifying their IP Addresses, SNMP Port Numbers, and the Manager's Community String.

6. Click OK when finished.



SNMP Trap Configuration

The Raritan Enterprise MIB can be accessed via the FAQ Support section on Raritan's web site (www.raritan.com).

1. Click on the View FAQ drop-down arrow and select the Dominion KX from the list.
2. When directed to the Dominion KX FAQ section, click on the first MIB query and then click on the link to view MIB file.

Trap name	Description
rebootStarted	The KX has begun to reboot, either through recycling power to the system or by a warm reboot from the OS.
rebootCompleted	The KX has completed its reboot.
userLogin	A user has successfully logged into the KX and authenticated.
userLogout	A user has successfully logged out of the KX properly.
userAuthenticationFailure	A user attempted to log in without a correct user name and/or password.
portConnect	A previously authenticated user has gained control of a particular KVM resource and begun a KVM control session.
portDisconnect	A user engaging in a KVM session closes the session properly.
userSessionTimeout	A user with an active session has experienced a session termination due to timeout.
userConnectionLost	A user with an active session has experienced an abnormal session termination.
portStatusChange	A new user record has been added to the KX user database.
userModified	A user record has been deleted.
groupAdded	A group record has been modified in the KX user database.
groupDeleted	A group record has been deleted.
startCCManagement	The device has been put under CC SG Management.
stopCCManagement	The device has been removed from CC SG Management.

Trap name	Description
factoryReset	The device has been reset to factory defaults.
deviceUpgradeStarted	The KX has begun updating itself via an RFP file.
deviceUpgradeComplete	The KX has completed updating itself via an RFP file.
KXPowerSupplyFailure	A power supply on a dual-power KX has failed.
userPasswordChanged	This event will signal if the password of any user within the product is modified.
networkFailure	One of the Ethernet interfaces of the product can no longer communicate over the network.

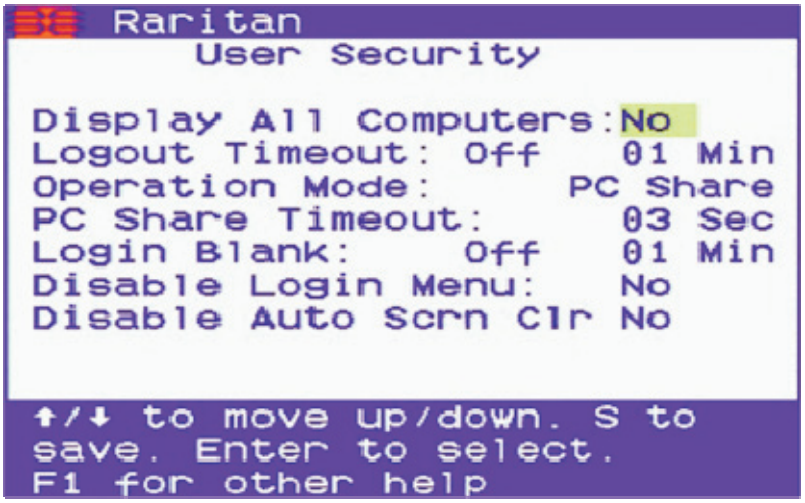
Chapter 4 Local Console Access

In This Chapter

When you are at the server rack, the Dominion KX provides standard KVM switch functionality via its Local Console, which feature onscreen display (OSD) for quick, convenient switching between servers. The Dominion KX Local Console provides a direct analog connection to your connected servers. Using the Local Console, the performance is same as if you were directly connected to the server's keyboard, mouse, and video ports.

Dominion's Local Console supports the following language keyboards: US, UK, German, and French (remote ports support US, US International, UK, German, French, and Japanese).

Important: By default, the KX sometimes sends a left-shift key to "wake up" targets from power-save or screen-save mode. However, on some targets this can interfere with BIOS entry during bootup. To disable this behavior, go to the User Security page and set the option "Disable Auto Scrn Clr" to Yes.



Physical Connections

Local Consoles connections can be found on the rear panel of the Dominion KX.

- Monitor: Attach a standard multisync VGA monitor to the HD15 (F) video port.
- Keyboard: Attach either a standard USB keyboard to one of the USB ports or a standard PS/2 keyboard to the Mini-DIN6 keyboard port.
- Mouse: Attach either a standard USB mouse to one of the USB ports or a standard PS/2 mouse to the Mini-DIN6 mouse port.
- Hubs: A USB keyboard and/or mouse can be also connected through a standard USB hub, which may be plugged into either USB port on the KX. A total of three external hubs are supported.
- Combo: If using a "combo" keyboard (a keyboard with a built-in mouse or trackball that attaches with a single USB cable), plug the USB connector into either USB port on the KX. Do not connect any other USB or PS/2 devices. Note that USB combo devices require KX 1.4.7 or later.

Note: Some combo devices (such as the Dell KVM drawer Model # 15FP) have a single USB connector as well as a PS/2 mouse connector.
When using a device like this, you may connect just the USB connecter (recommended, but requires KX 1.4.7 or later), or you may use the USB-to-PS/2 adapter supplied with the device to plug the USB connector into the purple PS/2 keyboard input on the KX, and plug the PS/2 mouse connecter into the green PS/2 mouse input on the KX (which will work on all versions of the KX, including legacy versions).

Note: USB ports are to be used only for keyboard, mouse and/or hub access. Other USB devices, such as external drives, scanners, etc. should not be connected to these ports.

Simultaneous Users

The Dominion KX Local Console provides an independent access path to your connected servers. Using the Local Console does not prevent users from simultaneously connecting over the network and, even when users have connected to the Dominion KX over the network, you may still simultaneously access your servers from the rack via the Local Console.

Security and Authentication

To use the Dominion KX Local Console, first authenticate with a valid user name and password. The Dominion KX provides a fully-integrated authentication and security scheme, whether you access the Dominion KX via the network or via the Local Console. In both cases, users use the same user name and password and the Dominion KX allows access only to those servers to which a user has access permissions (see ***Administrative Functions*** (on page 146) for additional information on creating server access and security settings).

If your Dominion KX has been configured for external authentication services (LDAP, Active Directory, or RADIUS), authentication attempts at the Local Console also are authenticated against the external authentication service.

Local Factory and Password Reset

If you forget the administrator password, there is currently no way to reset it to factory default to gain access. However, you can hard-reset a Dominion KX unit with this special user name and password, as described here.

- Type the user name admin and the password R*E*S*E*T. This password is case-sensitive.

This user name and password work only from your local access port. When working remotely, only the actual password assigned to administrator will gain access.

When this sequence is recognized, the device will not allow access as usual but will perform the specified reset action (Local Device Reset mode) as specified in the KX Manager Security Settings panel.

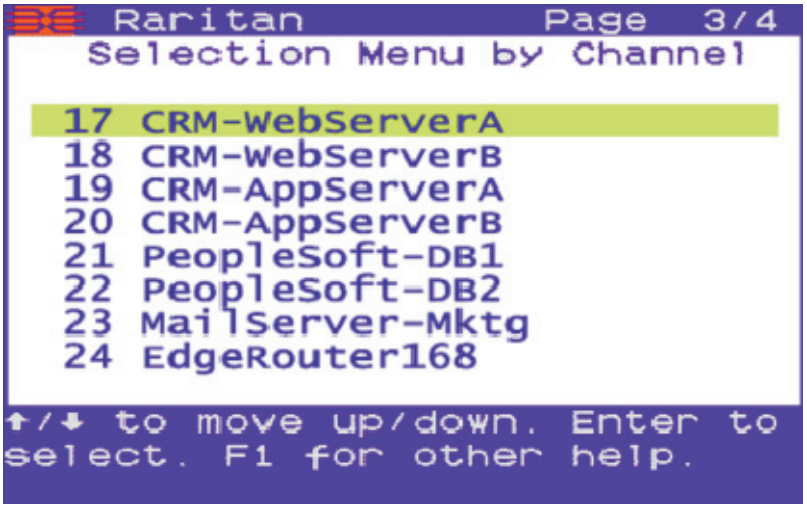
If Enable Local Factory Reset is performed, reset the network and other parameters from the local console and then reboot the Dominion KX unit.

Note: Passwords can consist of twenty (20) alphanumeric characters on the English keyboard, as well as the following symbols: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

Selecting Servers

Server Display Options

While you operate the Local Console, the Dominion KX will display a list of those servers to which you have permission to access.



Your servers can be sorted and displayed by two different parameters:

- Select by Channel: Press F2 while in the local console to display your servers listed in numerical order, as determined by the physical Dominion KX server port to which they are connected.
- Select by Name: Press F12 while in the local console to display your servers listed in alphabetical order by name.

Accessing a Server

While viewing the Server Display in the Local Console, press the up and down arrow keys to scroll through the list of servers. Eight servers are listed per page. If your list spans multiple pages, press the PgUp and PgDown keys to scroll between screens.

Select a server (when the server is highlighted with the yellow bar) you want to access and press Enter. The Local Console closes and you are connected directly to the server you have selected.

To return to the Local Console, press Scroll Lock twice rapidly.

Local Console Administration

The Dominion KX should ideally be managed via the Dominion KX Manager (see ***Administrative Functions*** (on page 146) for additional details). However, the Dominion KX Local Console provides access to select administrative functions. Only users with administrative privileges can access these functions, via the Administrative Functions menu.

Accessing the Local Console

➢ ***To select a server for controlling at the Local Console:***

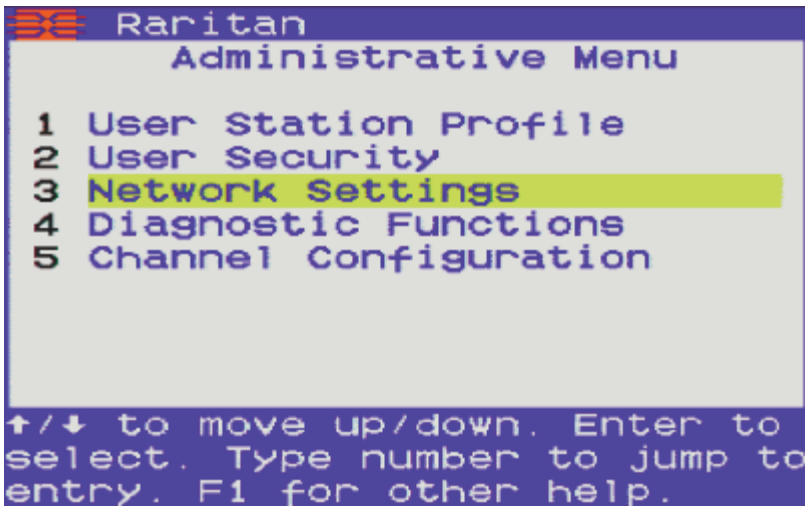
- If you are presently logged out of the Local Console: Type a valid user name and password, and the Locale Console appears.
- If a server is presently already selected: Press the Locale Console "Hot Key" Scroll Lock twice rapidly to access the Locale Console.

Important: The Local Console Hotkey is Scroll Lock, Scroll Lock (this combination can be changed via the Locale Console). Keep in mind that certain hot keys are reserved by the operating system, and you must not assign them to DKX functions.

Renaming Servers

Assign names to the servers connected to the Dominion KX from the Local Console while you are physically located next to the servers themselves.

1. Log in to the Dominion KX as a user with administrative privileges and press F5 to activate the Administrative Menu.



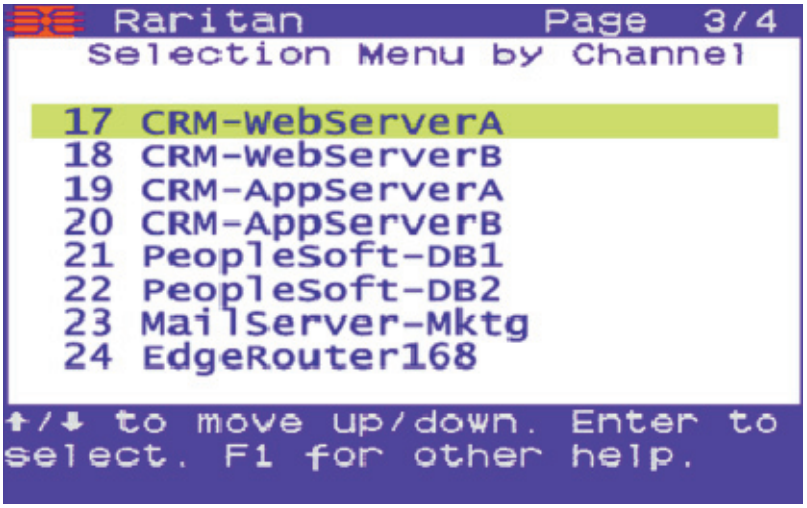
2. Choose Option 5, Channel Configuration. The Channel Configuration menu appears.

3. Use the up and down arrow keys to select a server port to rename and then press Enter.
4. When the highlighting turns green, type a name (up to 19 characters) to identify the server connected to that port.

5. Press Enter to save.

Server Display Options

While you operate the Local Console, the Dominion KX will display a list of those servers to which you have permission to access.



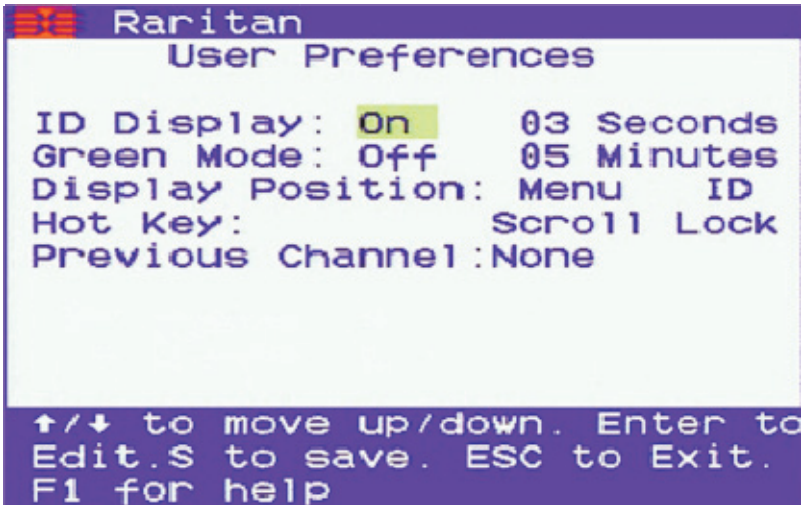
Your servers can be sorted and displayed by two different parameters:

- Select by Channel: Press F2 while in the Locale Console to display your servers listed in numerical order, as determined by the physical Dominion KX server port to which they are connected.
- Select by Name: Press F12 while in the Locale Console to display your servers listed in alphabetical order by name.

Setting Administrative User Preferences

The following preferences can be set for administrators:

- ID Display - this ID contains the name of the device in a pop-up. By default, the pop-up is displayed for 3 seconds when users hover over it but this can time can be changed as needed.
- Green Mode - this is the screensaver setting that is applied. The screensaver is set to come on after 5 minutes by default but can be changed as needed.
- Display Position - allows you to move the menu or the ID on the page.
- Hot Key - allows you to define your own hot key exit from a local connection to a target server. Once a hot key is assigned, it will be removed from the list of options so it cannot be applied to another channel. The possible choices are:
  - Scroll Lock
  - Left Alt
  - Left Shift
  - Caps Lock
  - Num Lock
- Previous Channel - if you have 2 channels defined, you can toggle between the current and previous channel.



Allowable Characters

The following characters are permitted in DCIM channel names:

Character	Description
Letters	Upper and lowercase a - z, A - Z
Numbers	0 - 9
Special characters	Minus ('-') plus ('+'), slash ('/'), period ('.') colon(':') space (' ')

Only these characters should be entered in the Locale Console due to hardware limitations in the Locale Console and CIMs. If other characters are entered, they will be blocked or changed to other valid characters. For example, underscore (_) should not be used. If it is entered, it will be changed by the Locale Console to the letter M.

Changing Network Settings

The Network Settings menu contains the following:

- Name (of network)
- IP Address
- Subnet Mask IP
- Gateway Address
- MAC Layer Parameters
- Autonegotiation (IPs)

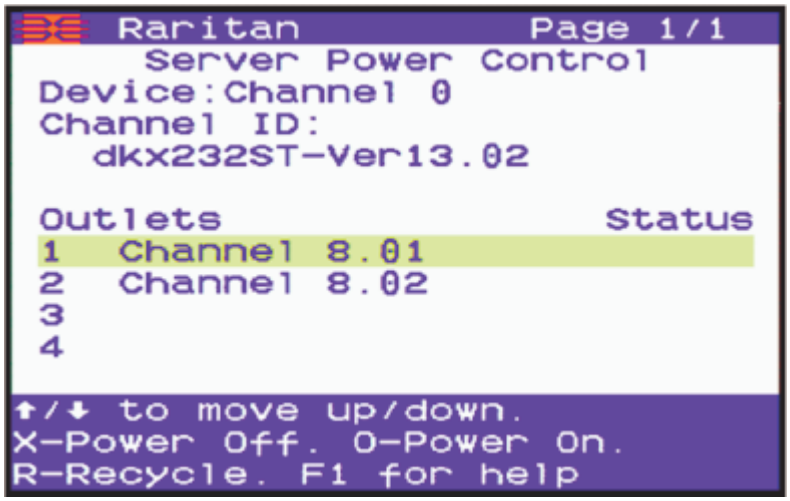
1. To acquire the speed and duplex automatically, leave the Autonegotiate option set to Yes. If the option is set to No, you will be able to set the following preferences:
   - Speed (10 or 100)
   - Duplex (half or full)
2. Log in to the Dominion KX as a user with administrative privileges, and press F5 to activate the Administrative Menu.
3. Choose Option 3, Network Settings. The Network Settings menu appears.
4. Use the up and down arrw keys to navigate through the menu. To edit a setting, press Enter. When the highlight turns green, that setting can be edited; use numerical keys as well as the á and â arrow keys to change values.
5. Press S to save changes, and then press Esc to exit the menu. This will cause the KX to reboot.

Important: Dominion KX must be rebooted for new network settings to take effect.

Power Management

Control channels with power associations on the Locale Console using the F3 key. If you select a channel without a power association, a No Outlet/Access Denied message appears at the base of the Channel Configuration menu.

1. From the Channel Configuration menu, choose the channel to turn off, turn on, or recycle power to and press the F3 key. The Server Power Control page appears.
2. Use the up and down arrow keys to choose a channel.
3. Press the letter X to power Off the channel.
4. Press the letter O to power On the channel.
5. Press the letter R to Recycle power to the channel.



6. When finished, press Esc to return to the Channel Configuration menu.

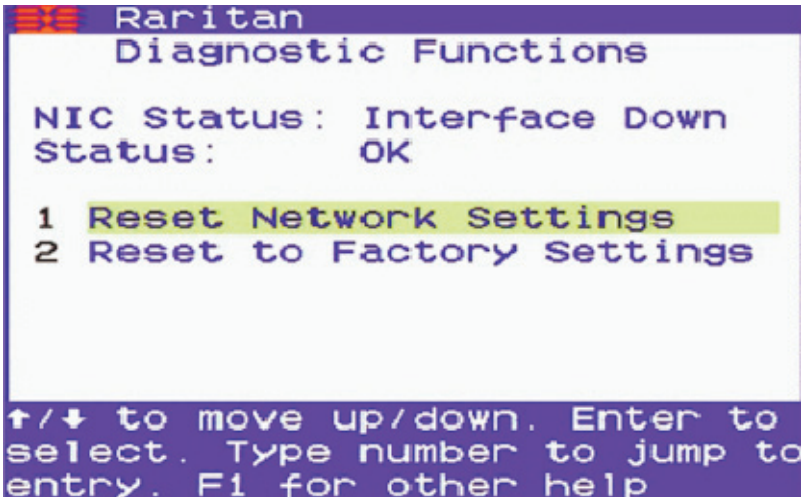
Diagnostic Functions

The Diagnostic Functions menu contains the following information and options:

- NIC Status - network specific and cannot be changed.
- Status - current status of the network that is specific to your network and cannot be changed.
- Reset to Network Settings - resets to the original network settings.
- Reset to Factory Settings - select to set the KX back to its original, factory settings.

➢ ***To access the Diagnostic Functions menu:***

1. Log in to the Dominion KX as a user with administrative privileges and press F5 to activate the Administrative Menu.
2. Choose Option 4, Diagnostic Functions. The Diagnostic Functions page appears.

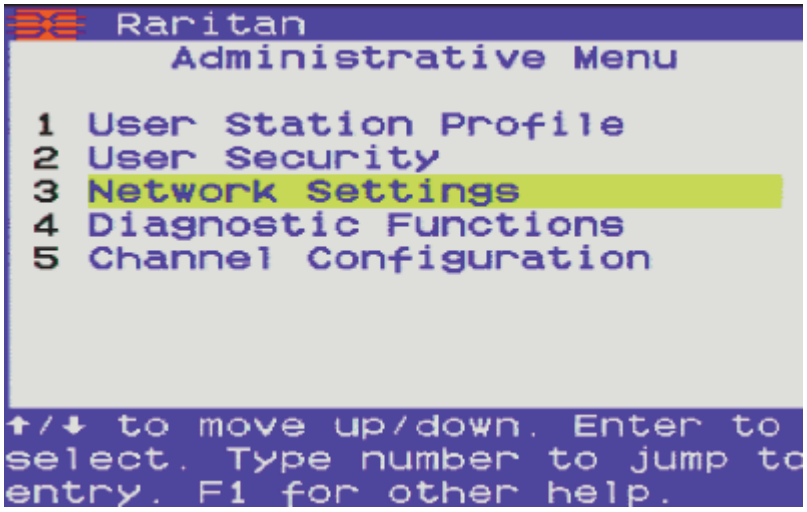


Setting Session Timeout

Session timeouts apply only to local users. When the local user is viewing target video and there is no keyboard or mouse activity for a specified amount of time, that user is logged out of the target video but the Locale Console remains active.

Note: Do not confuse a session timeout with an idle user timeout, which applies to all users whether local or remote. When idle user timeout expires, the user is disconnected from the video and also logged out of the client application (the Locale Console, MPC, or RRC).

1. Log in to the Dominion KX as a user with administrative privileges and press F5 to activate the Administrative Menu.

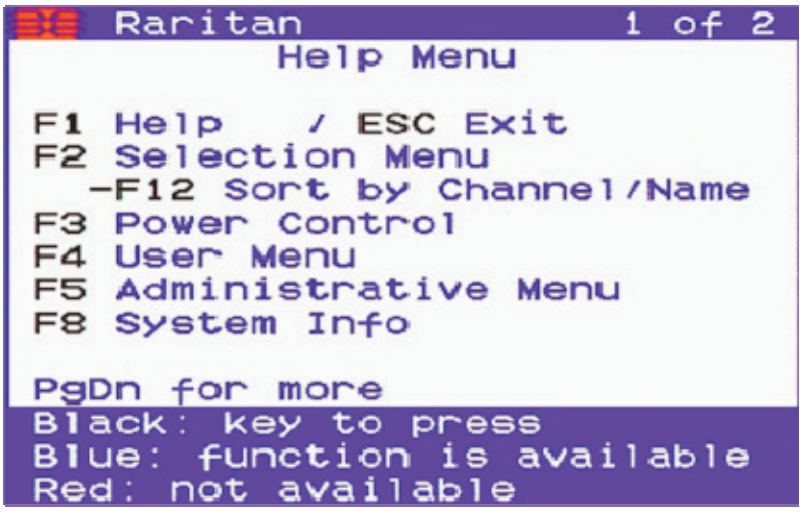


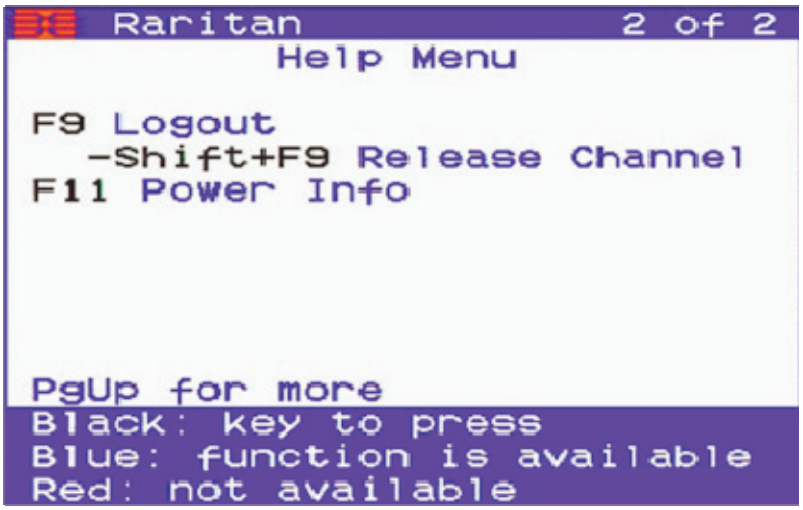
2. Choose Option 1, User Station Profile. The User Station Profile page appears.

3. Use the up and down arrow keys to navigate through the menu to the Session Timeout field.
4. Press Enter.
5. When the highlighting turns green, use numerical keys or the up and down arrow keys to change the values. By default, the session timeout feature is set to 00 minutes, which means there is no timeout and users are never logged off for inactivity. You can set a timeout period in one minute increments, up to a maximum of 30 minutes.
6. Press S to save changes and then press Esc to exit the menu.

Help Menu

- To access the Help menu for the Dominion KX Local Console, press F1. The Help menu, which consists of 2 (two) pages, appears.

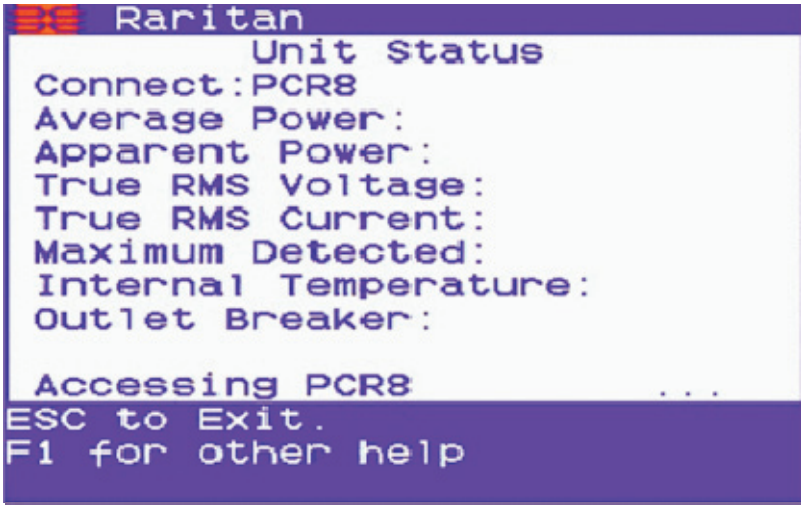




Power Information

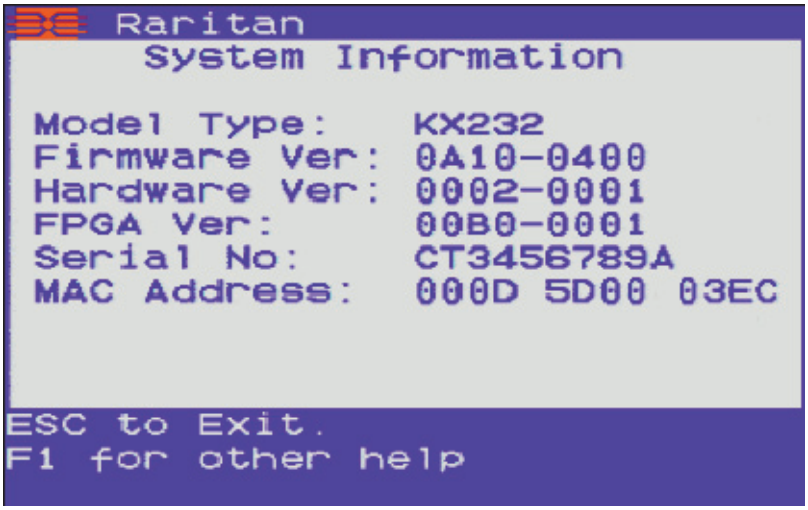
You are able to access information on the power status of a power strip from the Help menu by pressing the F1 key, paging down to page 2 of the Help menu, and then pressing F11. The Power Info page provides the following power related information for the power strip:

- Connect - connection being monitored.
- Average Power - average power of the unit.
- Apparent Power - volts x amps (VA).
- True RMS Voltage - the parameters of the RMS voltage.
- True RMS Current - the parameters of the RMS current.
- Maximum Detected - maximum detected current.
- Internal Temperature - the internal temperature of the KX.
- Outlet Breaker - status of the power strip breaker (Good or Fault). If Fault is displayed, the power strip does not have a breaker.



Hardware/Firmware Information

If you need hardware and firmware information specific to your Dominion KX unit, log into the Local Console of your Dominion KX unit and press F8. The System Information page appears.



The Dominion KX firmware version 1.4 operates on all Dominion models:

- DKX116
- DKX132
- DKX216
- DKX232
- DKX416
- DKX432
- DKX464.

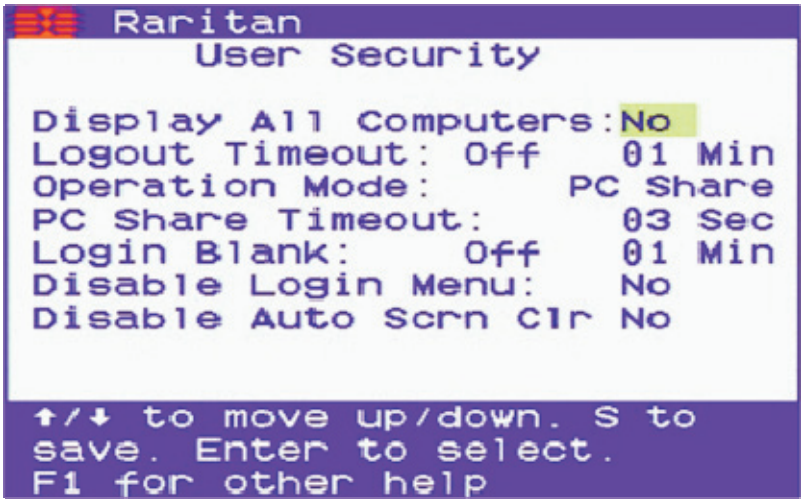
To determine the firmware upgrade version on an existing KX device in order to upgrade the firmare from the Raritan website (www.raritan.com) in the Firmware Upgrades section, choose the System Information command on the Setup menu in KX Manager or press the F8 key from the Locale Console to display the current firmware version.

Firmware version	KX firmware upgrade
0A28	Version 1.0
0A34	Version 1.0.3
0A47	Version 1.1

Firmware version	KX firmware upgrade
0B12	Version1.2
0B1B	Version 1.3
0B20	Version 1.4
0B2W	Version 1.4.1
0B33	Version 1.4.2
3C01	Version 1.4.5
3C03	Version 1.4.6
3C0E	Version 1.4.7

Local User Security Settings

1. Log in to the Dominion KX as a user with administrative privileges and press F5 to activate the Administrative Menu.
2. Choose Option 2, User Security. The User Security menu appears.



3. To disable login and logout, set the Disable Login Menu option to Yes. This will cause the KX to reboot and the Local Console will automatically log in to the channel selection menu. This puts the Locale Console into Administrator mode.
4. To display all computers, enter *Yes* in the Display All Computers field. To display only active ones (the default), enter No in the field.

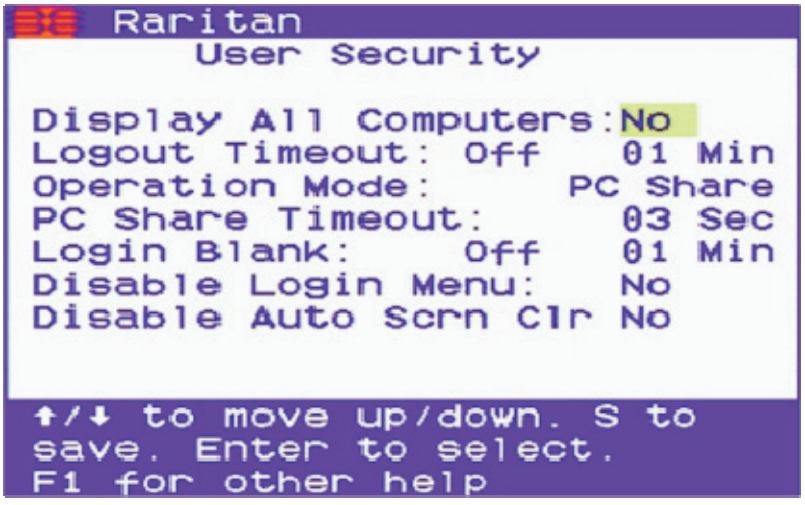
5. To set a logoff timeout, enter On and then enter the number of minutes for the timeout period in the Logoff Timeout field.
6. Select an operation mode in the Operation Mode field. The default is PC Share.
7. Enter a period of time for the login to remain blank in the Login Blank field. The default is 1 minute.
8. Press S to save changes and then press Esc to exit the menu.

Disable Auto Screen Clear Option

Important: The option that allows the Local Console to disable the default behavior of sending the left shift key to the target server to "wake up" servers in power saver mode or that have a screen saver running must be disabled.

To disable this behavior, set the Disable Auto Scrn Clr option on the User Security page to Yes. This is advised if this key sequence is interfering with BIOS entry.

1. Log in to the Dominion KX as a user with administrative privileges and press F5 to activate the Administrative Menu.
2. Choose Option 2, User Security. The User Security menu appears.
3. Set the Disable Auto Scrn Clr option to Yes.



Appendix A Specifications

In This Chapter

Digital KVM Switches

Part number	Product weight	Product dimensions (W x D x H)	Power
DKX116	8.65 lb 3.92 kg	17.3" x 11.4" x 1.75" 439 mm x 290 mm x 44 mm	100V/240V 47/63Hz 0.6A
DKX132	9.0 lb 4.1 kg	17.3" x 11.4" x 1.75" 439 mm x 290 mm x 44 mm	100V/240V 50/60Hz 0.6A
DKX216	8.65 lb 3.92 kg	17.3" x 11.4" x 1.75" 439 mm x 290 mm x 44 mm	100V/240V 50/60Hz 0.6A
DKX232	9.0 lb 4.08 kg	17.3" x 11.4" x 1.75 439 mm x 290 mm x 44 mm	100V/240V 50/60Hz 0.6A
DKX416	9.0 lb 4.08 kg	17.3" x 11.4" x 1.75" 439 mm x 290 mm x 44 mm	100V/240V 50/60Hz 1A
DKX432	9.5 lb 4.3 kg	17.3" x 11.4" x 1.75" 439 mm x 290 mm x 44 mm	100V/240V 50/60Hz 1A
DKX464	13.73 lb 6.24 kg	17.3" x 11.4" x 3.5" 439 mm x 290 mm x 90 mm	Dual Power 100V/240V 47/63Hz 1.8A

Computer Interface Modules (CIMs)

Part number	Product weight	Product dimensions (W x D x H)
DCIM-PS2	0.2 lbs 0.09 kg	1.3" x 3.0" x 0.6" 33 mm x 76 mm x 15 mm
DCIM-USBG2	0.2 lbs 0.09 kg	1.3" x 3.0" x 0.6" 33 mm x 76 mm x 15 mm
DCIM-SUSB	0.2 lbs 0.09 kg	1.3" x 3.0" x 0.6" 33 mm x 76 mm x 15 mm
DCIM-SUN	0.2 lbs 0.09 kg	1.3" x 3.0" x 0.6" 33 mm x 76 mm x 15 mm

Remote Connection

- Network: 10BASE-T, 100BASE-TX Ethernet
- Modem: Dedicated modem port (DB9M) for an external serial modem that is qualified for use with an US Robotics external serial modems. This information is accurate as of press date of this guide.
- Protocols: TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP

Raritan Remote Client (RRC) Applet

- Operating System Requirements: Windows XP/2000 with DirectX.

Windows NT support for some international keys are limited due to limited Microsoft support for DirectX on the Windows NT platform.

Dominion KX Manager (Remote Administration Applet)

For consistent operation across multiple operating systems and web browsers, Sun Java Runtime Environment (JRE) version 1.4.2_05 is used. If this version is not installed on the desktop client, your system will prompt you to install it.

TCP Ports Used

Port	Description
HTTP, Port 80 (optional)	All requests received by the Dominion KX via HTTP (port 80) are automatically forwarded to HTTPS for complete security. The Dominion KX responds to Port 80 for user convenience, relieving users from having to explicitly type "https://" in the URL field to access the Dominion KX, but while still preserving complete security.
HTTPS, Port 443 (optional)	This port is used for a single purpose only: to send the Dominion KX web-accessible clients (Raritan Remote Client and Dominion KX Manager) to the user. No other communication occurs on this port. If you do not wish to use the Dominion KX's web-access capabilities and instead prefer to use the installed client software provided on CD-ROM, you can prevent access to Port 443 via your firewall and the Dominion KX can still function.
Dominion KX (Raritan KVM Over IP) Protocol, Configurable Port 5000	With the exception of HTTP Port 80 and HTTPS Port 443, all communication to the Dominion KX occurs over a single, configurable TCP port. By default, this is set to Port 5000, but you may configure it to use any TCP port of your choice (except 80 and 443). For details on how to configure this setting, see ***Administrative Functions*** (on page 146).
SNTP (Time Server) on Configurable UDP Port 123 (optional)	The Dominion KX offers the optional capability to synchronize its internal clock to a central time server. This function requires the use of UDP Port 123 (the standard for SNTP), but can also be configured to use any port of your designation.

Port	Description
LDAP on Configurable Ports 386 and 636 (optional)	If the Dominion KX is configured to remotely authenticate user logins via the LDAP protocol, ports 386 and 636 will be used, but the system can also be configured to use any port of your designation.
RADIUS on Configurable Port 1812, 1645, or custom port (optional)	If the Dominion KX is configured to remotely authenticate user logs in via the RADIUS protocol, either port 1812 or 1645 will be used, but the system can also be configured to use any port of your designation.
RADIUS Accounting on Configurable Port	If the Dominion KX is configured to remotely authenticate user logins via the RADIUS protocol, and also employs RADIUS accounting for event logging, an additional port of your designation will be used to transfer log notifications.
SYSLOG on Configurable UDP Port 123 (optional)	If the Dominion KX is configured to send messages to a Syslog server, then the indicated port(s) will be used for communication - uses UDP Port 514.
SNMP Default UDP Ports (optional)	Port 161 is used for inbound/outbound read/write SNMP access and port 162 is used for outbound traffic for SNMP traps.

Target Server Connection Distance and Video Resolution

- Keyboard: PS/2 or USB
- Mouse: PS/2 or USB
- Video: VGA

Dominion KX models	Linux servers: DCIM-PS2, USB	Windows servers: DCIM-PS2/USB	SUN Solaris: DCIM-SUN/SUSB
KX116 KX132 KX216 KX232	75 to 150 ft 19.5 to 45 m	50 to 100 ft 15 to 30 m	50 to 75 ft 15 to 19.5 m
KX416 KX432 KX464	75 to 150 ft 19.5 to 45 m	75 to 150 ft 19.5 to 45 m	75 to 150 ft 19.5 to 45 m

Generally, distances closer to the lower range will provide excellent video quality in most environments. Distances towards the upper end of the range should show acceptable quality, but in some environments degradation of the video signal may start to appear.

The maximum supported distance is a function of many factors including the type/quality of CAT5 cable, server type, and server manufacturer, the video driver and monitor, environmental conditions and user expectations.

The KX416 and KX432 models provided enhanced video signal quality at longer distances across the three types of servers tested. For maximum distance, utilize one of the KX4 models.

The use of Paragon CIMs will not increase the distance between the KX and the target server.

Due to the multiplicity of server manufacturers and types, OS versions, video drivers, etc. and the subjective nature of video quality, Raritan cannot guarantee performance across all distances in all environments.

Supported Video Resolutions

Resolutions		
640x480 @ 60Hz	800x600 @ 56Hz	1024x768 @ 60Hz
640x480 @ 72Hz	800x600 @ 60Hz	1024x768 @ 70Hz
640x480 @ 75Hz	800x600 @ 72Hz	1024x768 @ 75Hz
640x480 @ 85Hz	800x600 @ 75Hz	1024x768 @ 85Hz
720x400 @ 70Hz	800x600 @ 85Hz	1152x864 @ 60Hz

Resolutions		
720x400 @ 85Hz		1152x864 @ 70Hz
		1152x864 @ 75Hz
		1280x960 @ 60Hz
		1280x1024 @ 60Hz

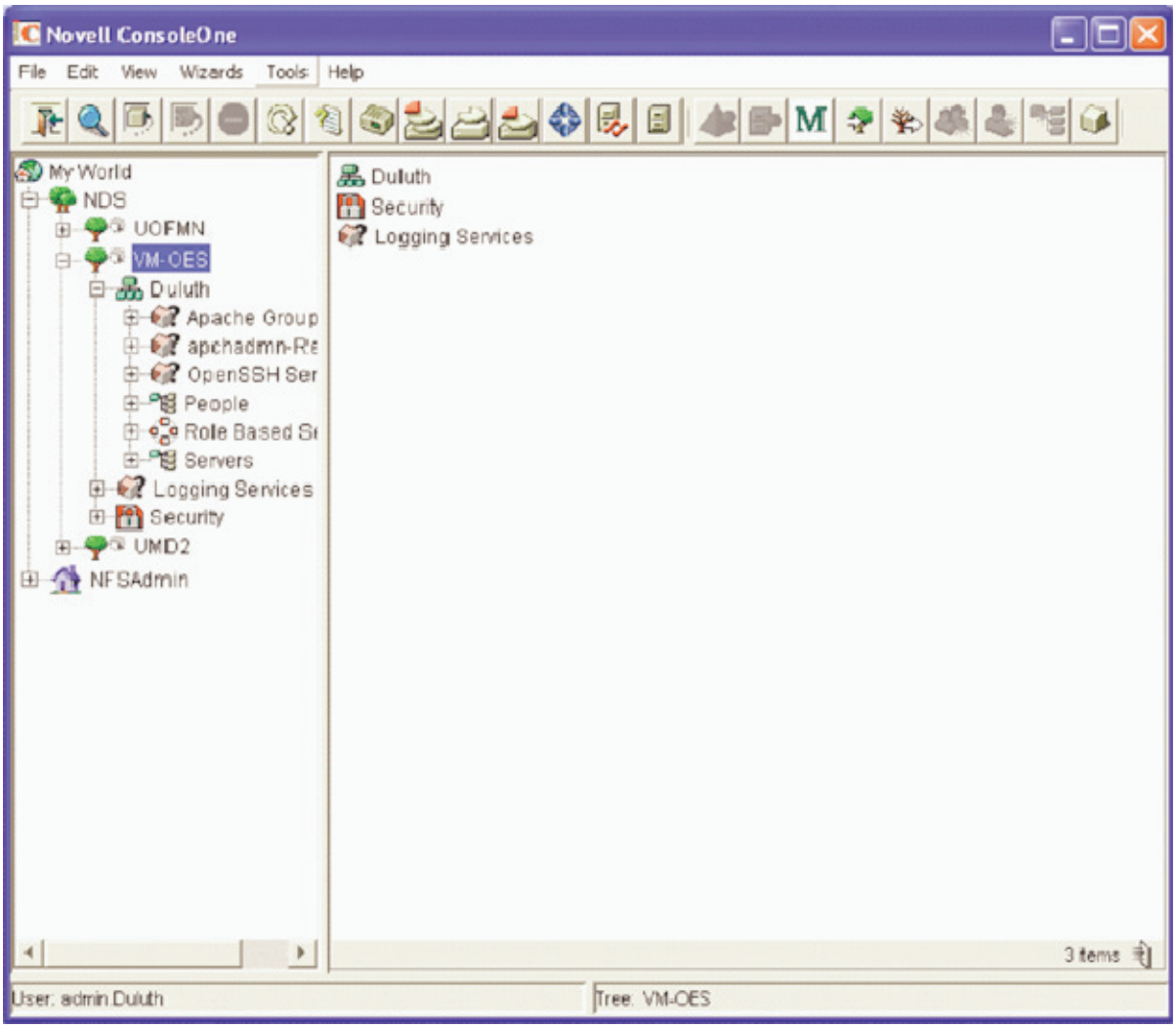
Certified Modems

- US Robotic 56K Fax and Modem
- ZOOM v90; RS232 interface
- ZOOM v92; RS232 interface
- USR (US Robotic) Sportster 56K v90
- USR (US Robotic) Courier 56K v90
- Trust 56K V.92 External Modem

Appendix B Novell eDirectory

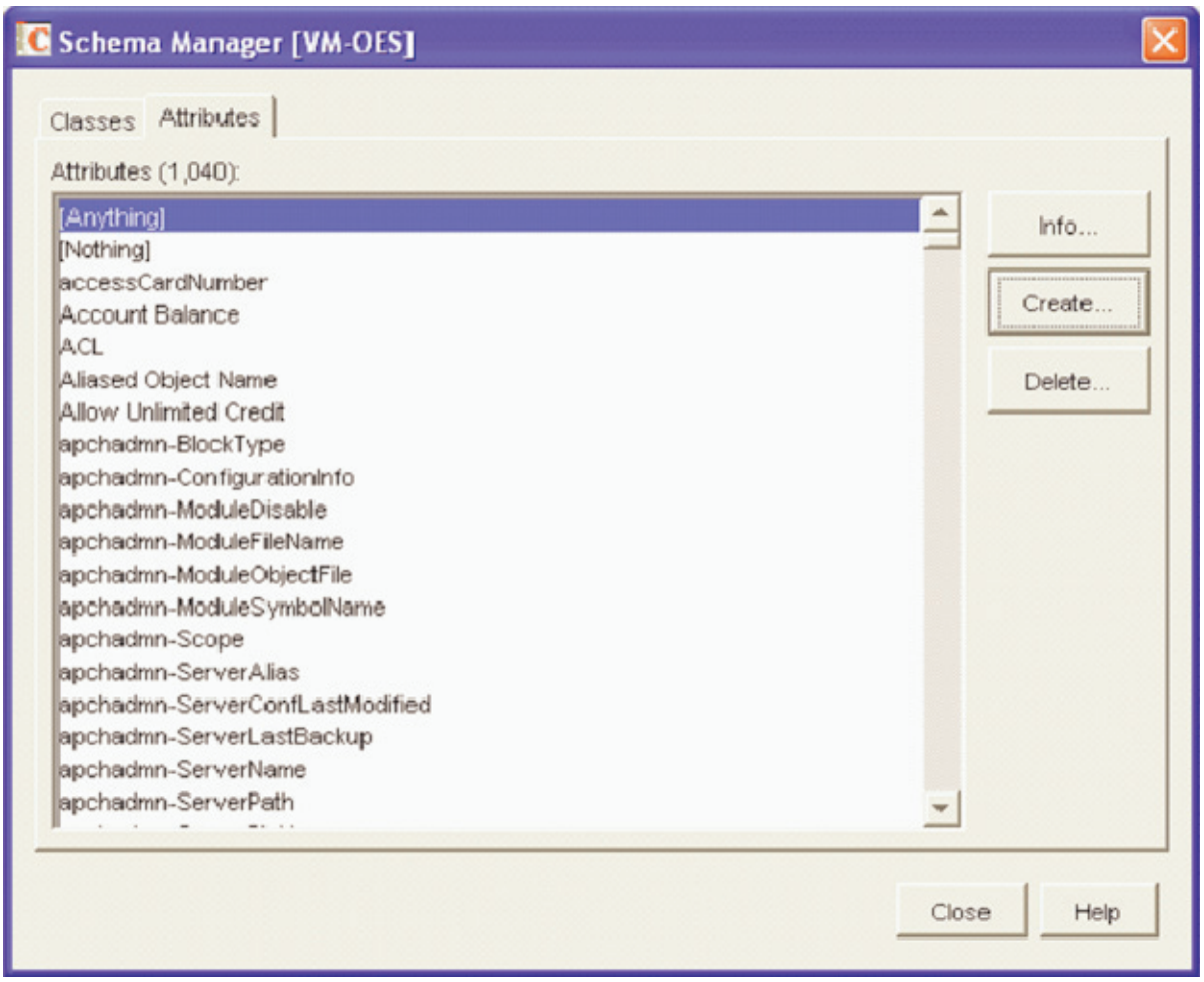
This information is offered as an overview of Novell's eDirectory. For more detailed information, visit Novell's website.

1. Log in to the tree with Admin rights to [Root], or some equivalent that has rights to modify the schema of eDirectory. Open Console One and select your tree in the left panel.

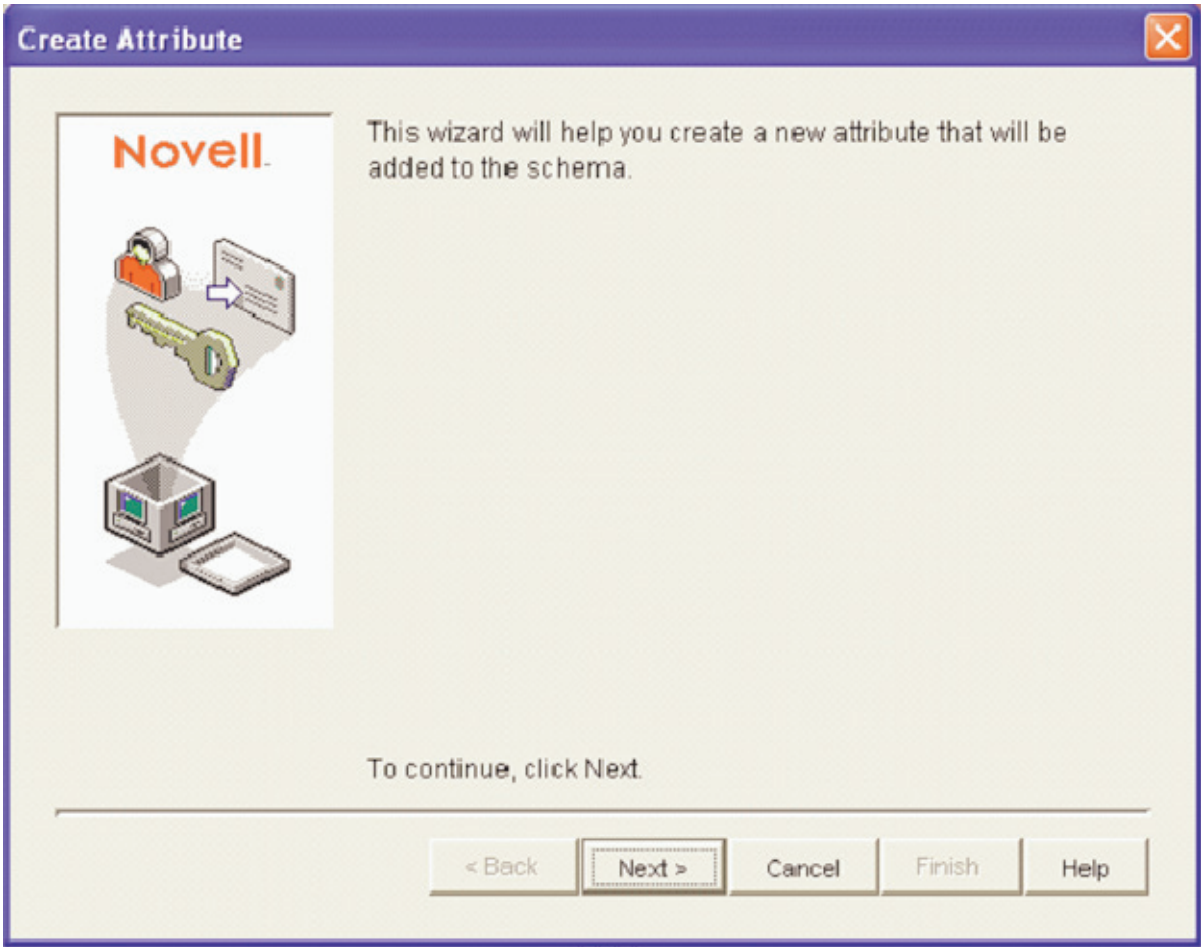


2. On the Tools menu, choose Schema Manager.

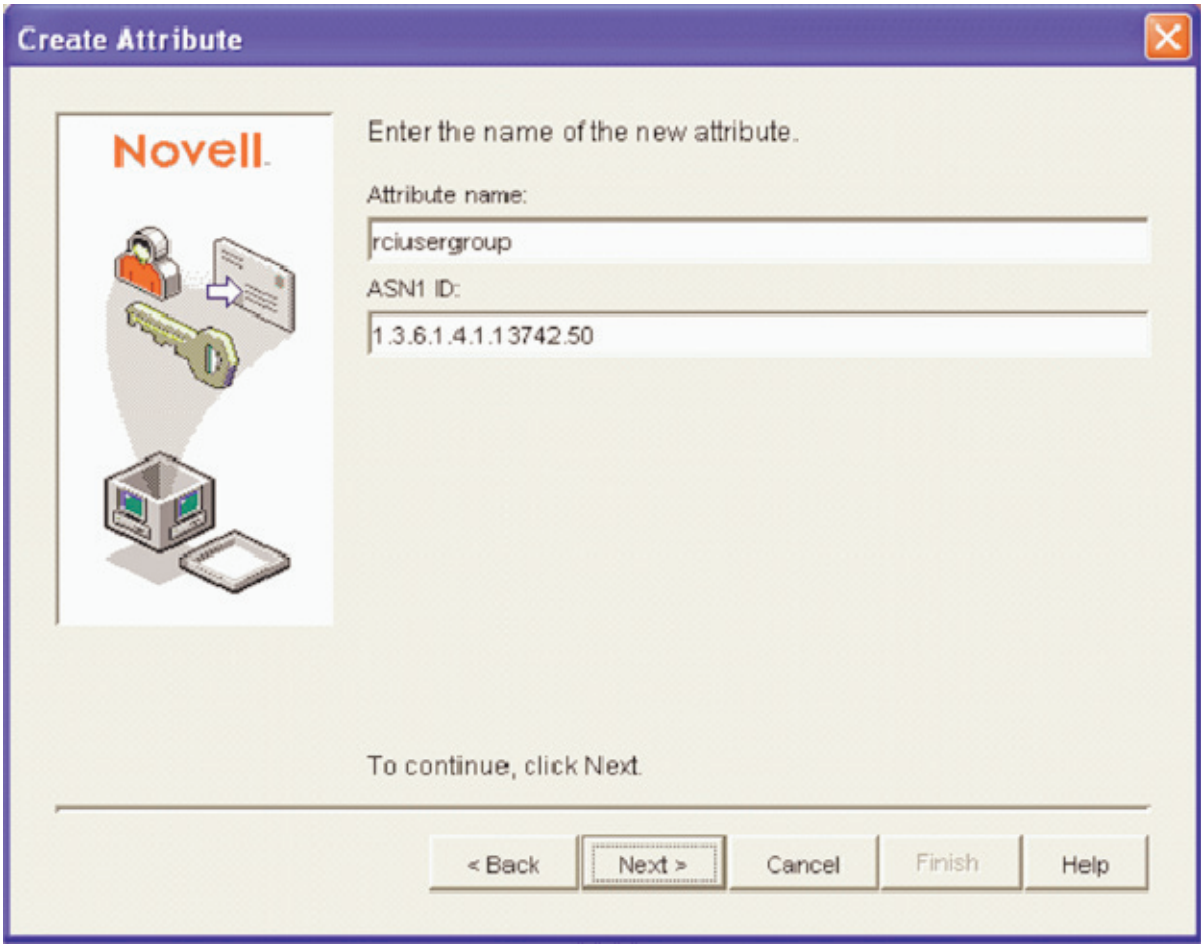
3. In the Schema Manager window, click on the Attributes tab, then create Create to create a new attribute.



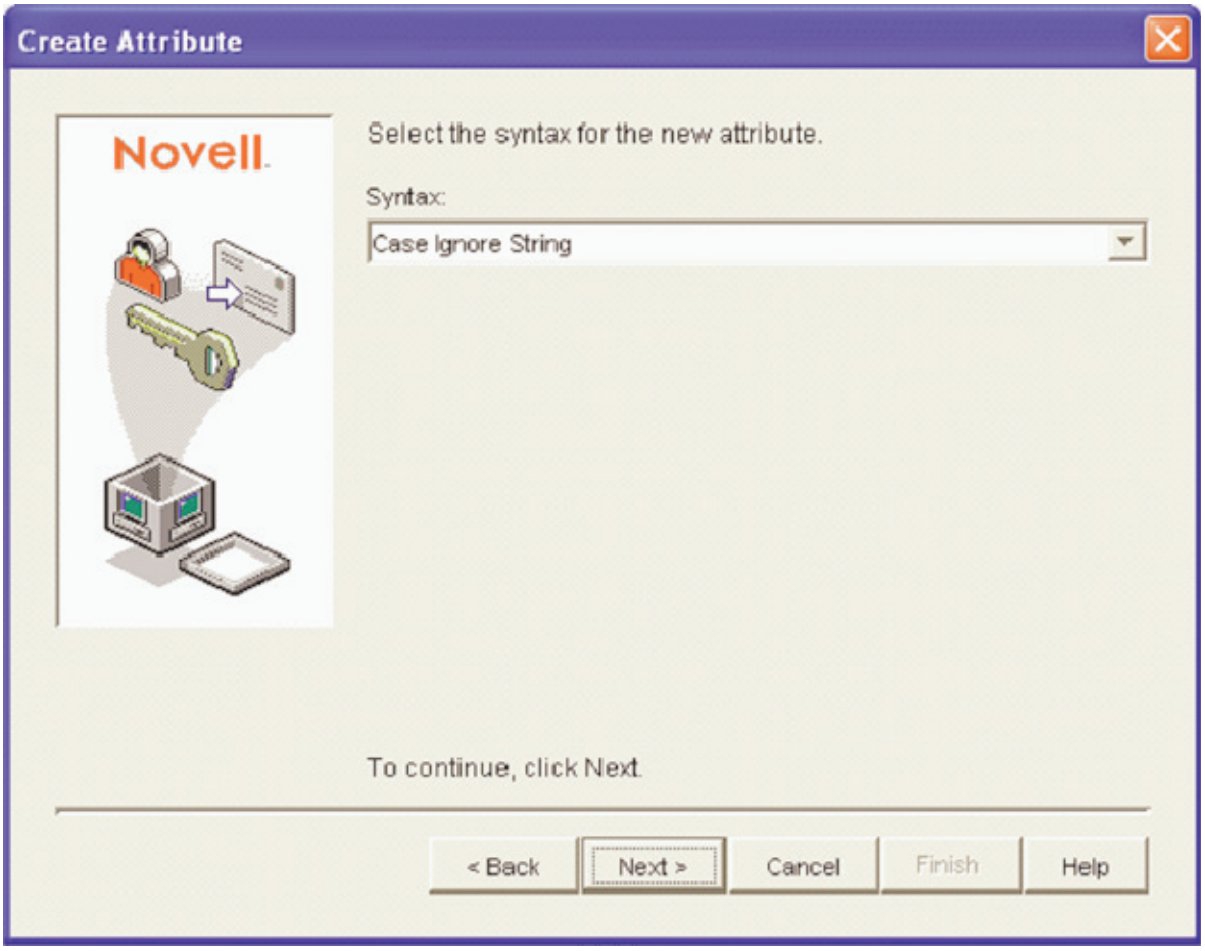
4. Console One will launch the Create Attribute Wizard. Click Next.



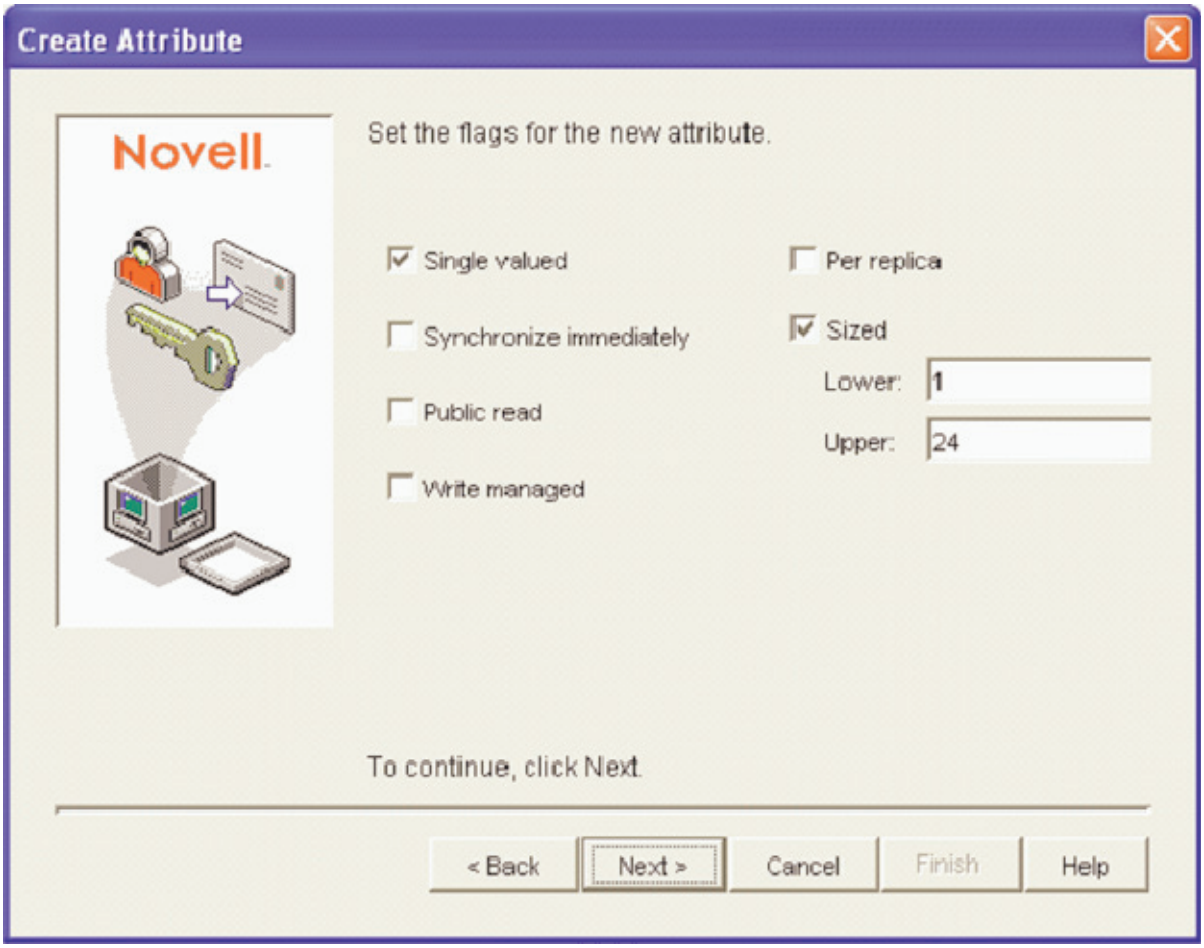
5. Type `rciusergroup` in the Attribute name field and type *1.3.6.1.4.1.13742.50* in the ASN1 ID field. Click Next.



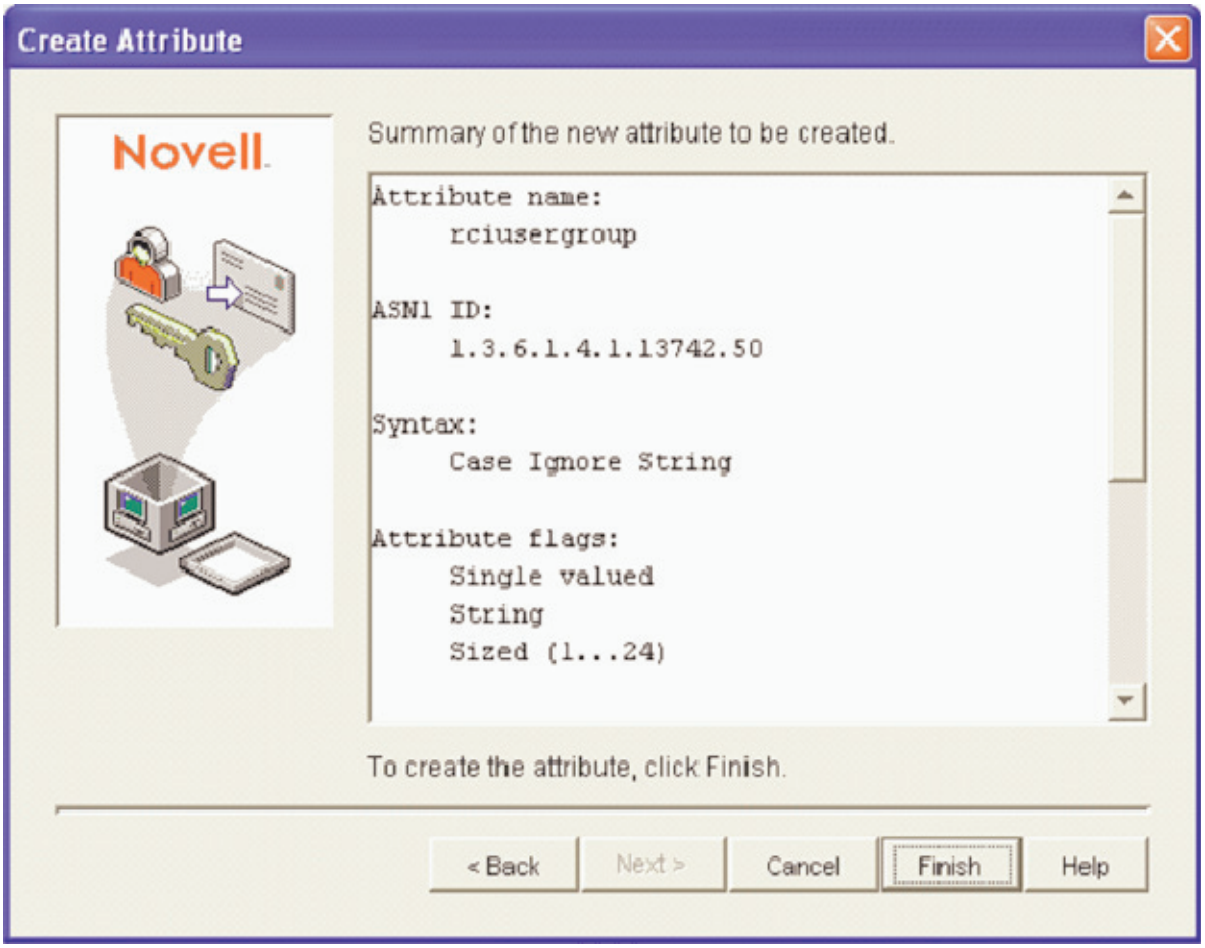
6. Click on the Syntax drop-down arrow and select Case Ignore String from the list. Click Next.



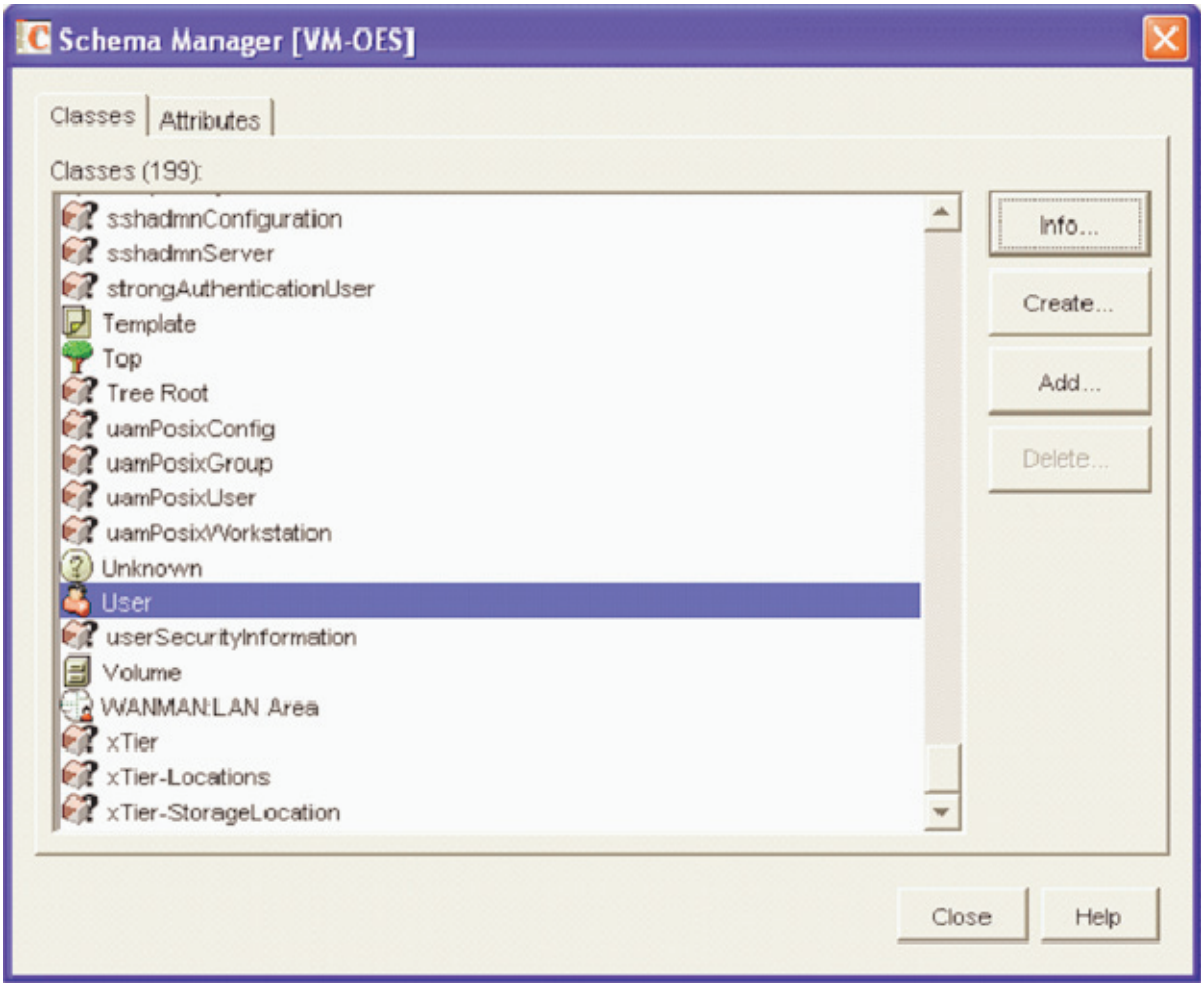
7. Click on the checkboxes before Single valued and Sized to set those flags. Type 1 in the Lower field and type *24* in the Upper field. Click Next.



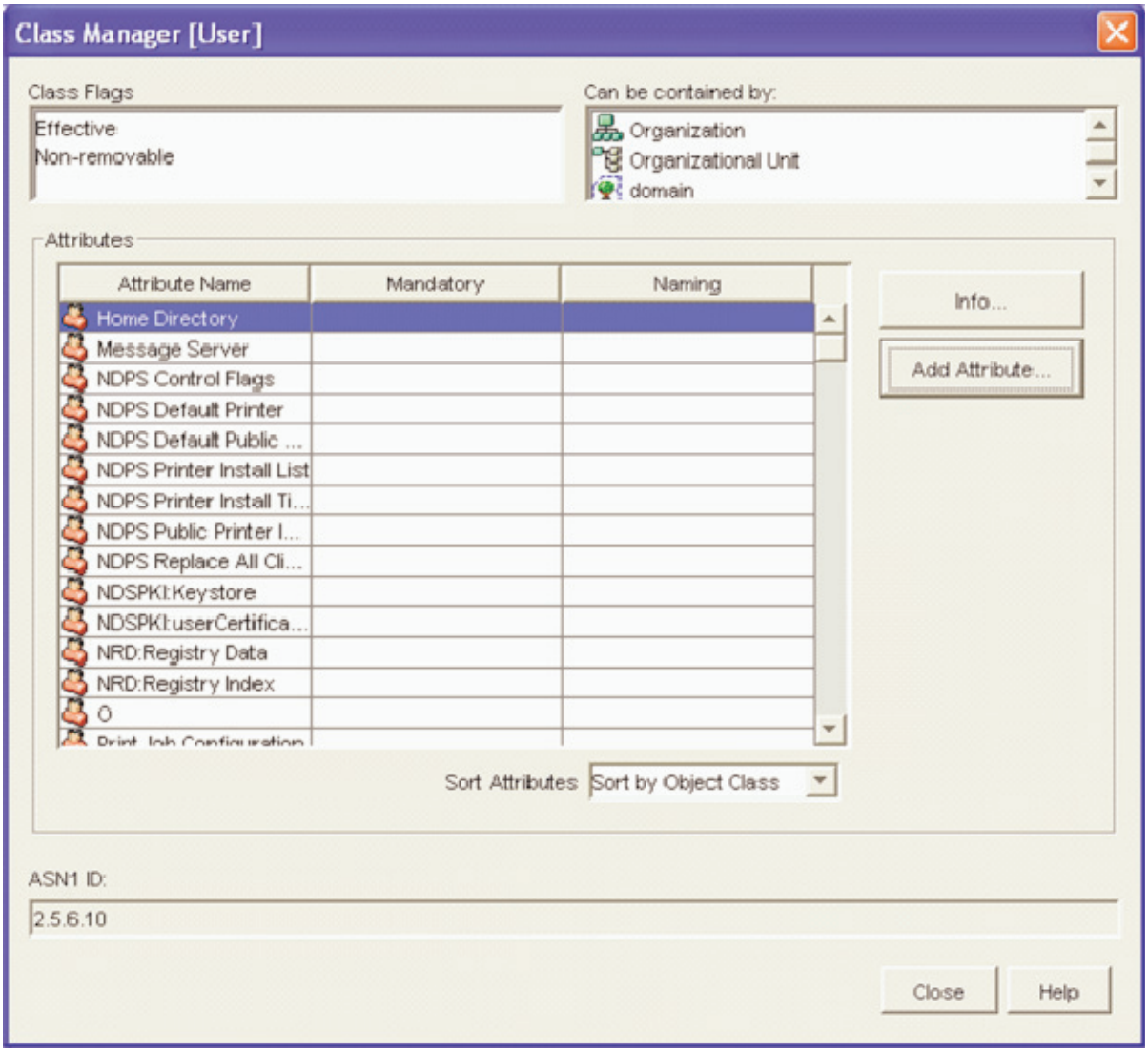
8. A Summary dialog displaying your data appears. Click Finish to create the attribute in eDirectory, or click Back to return to previous screens and change your data.



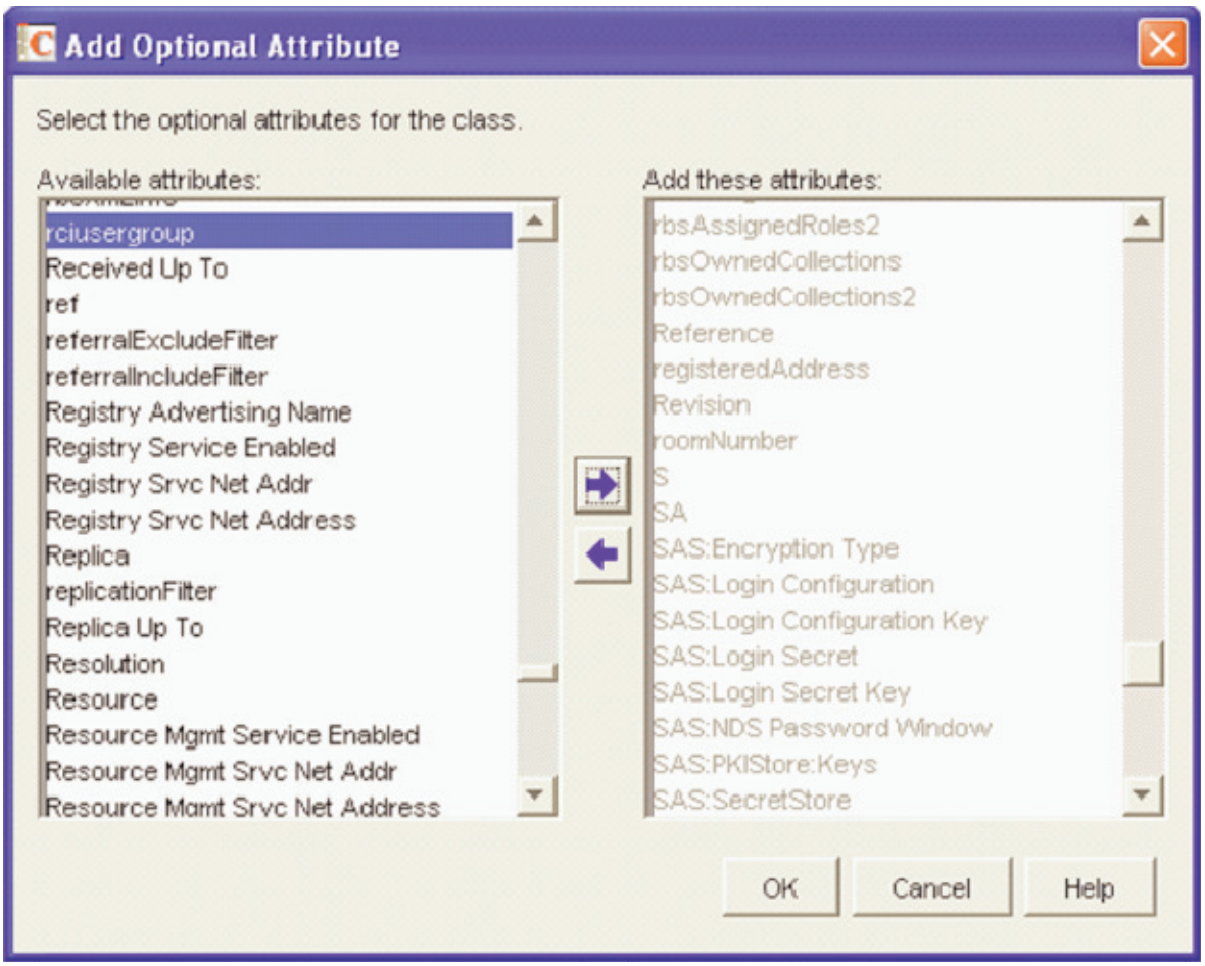
9. When you finish, you return to the Schema Manager dialog.



10. Click on the Classes tab, select the User class, and click Info. The Class Manager dialog appears.

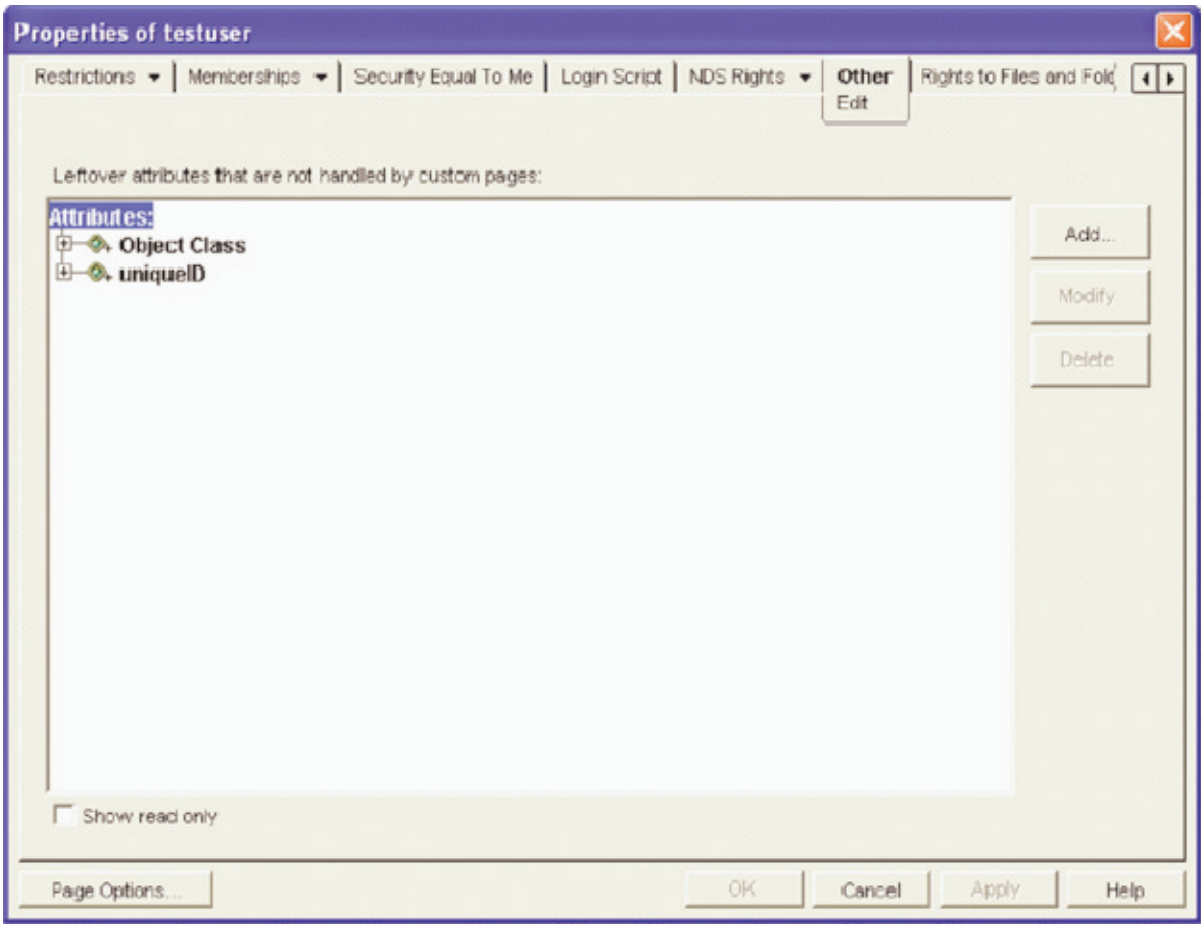


11. Click Add Attribute to add the rciusergroup attribute to the User class. The Add Optional Attribute window appears.

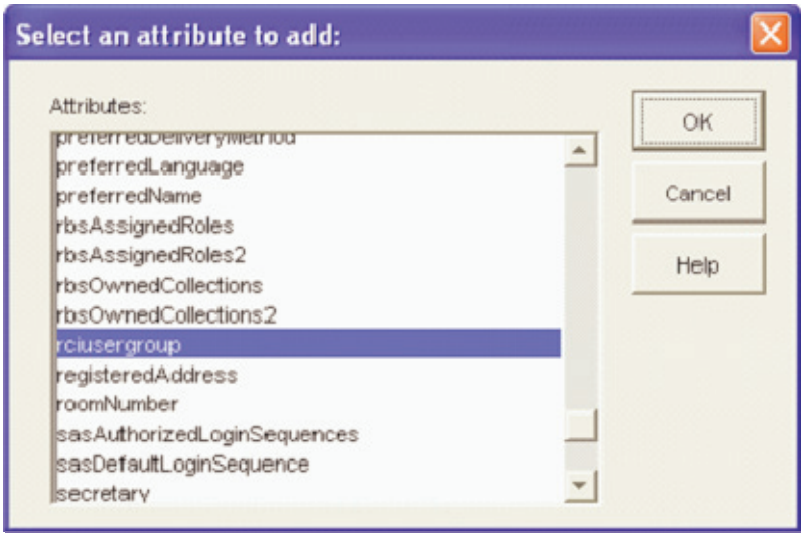


12. Select rciusergroup in the Available attributes pane on the left, and then click the blue arrow à to add the attribute to the Add these attributes pane on the right. Click OK.
13. Click Close and in the next dialog, click Close once more to return to the main Console One dialog.
14. Important: Ensure that you want to change this attribute; this is a permanent change.

15. Add a value to the attribute using Console One, LDIF operations with ICE, or ldapmodify (note that these are outside scope of this document). If using Console One, right-click on the user object and click Properties. Click on the Other tab to add attribute and value for rciusergroup.

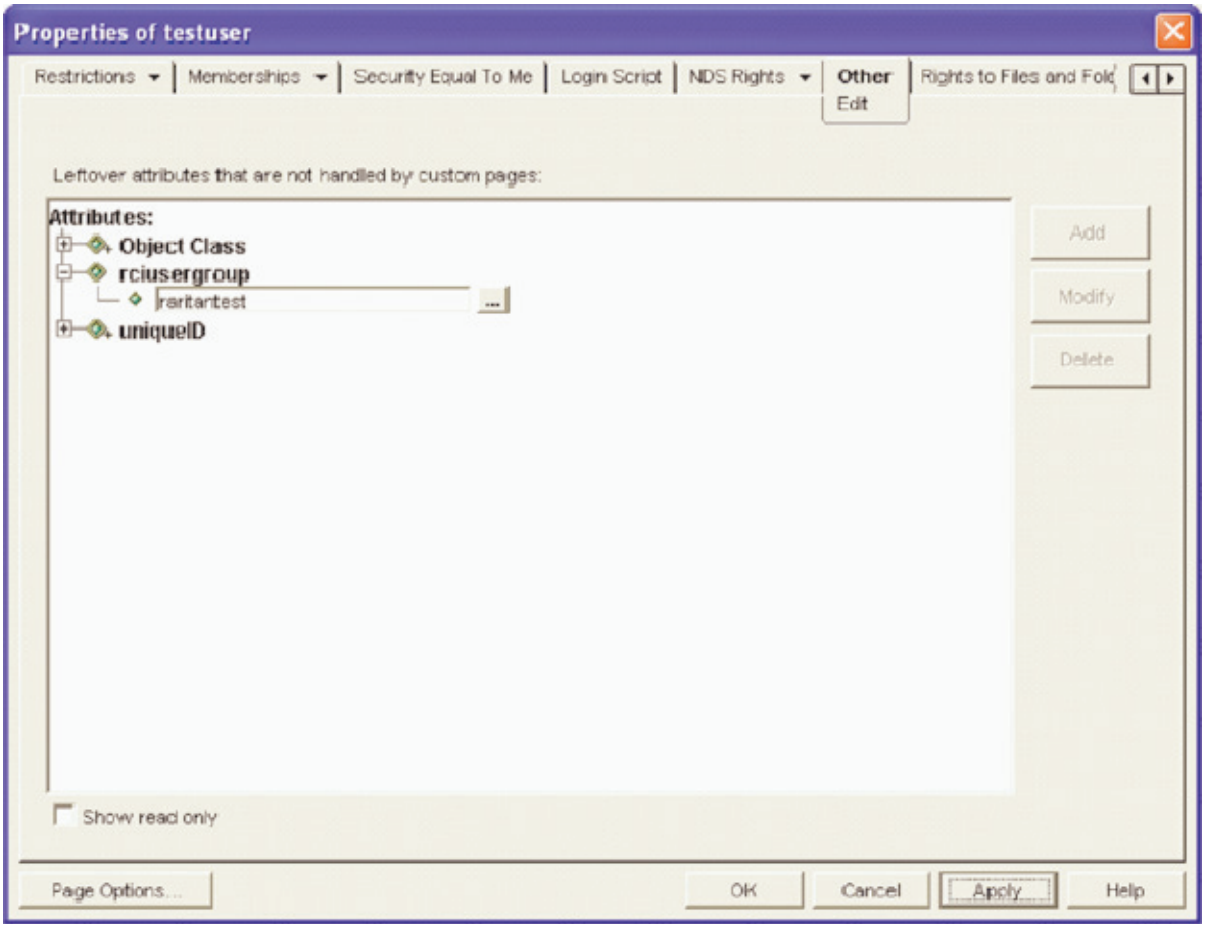


16. Click Add.

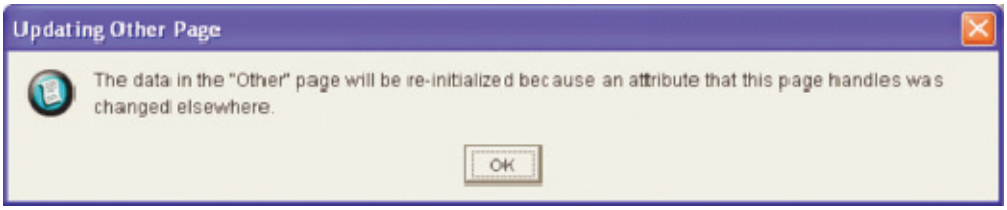


17. Select the rciusergroup attribute and click OK to add the attribute to your User object.

18. When you return to the Properties dialog, rciusergroup appears in the Attributes tree. Type the name of the User Group you created on the Dominion KX device and then click Apply.

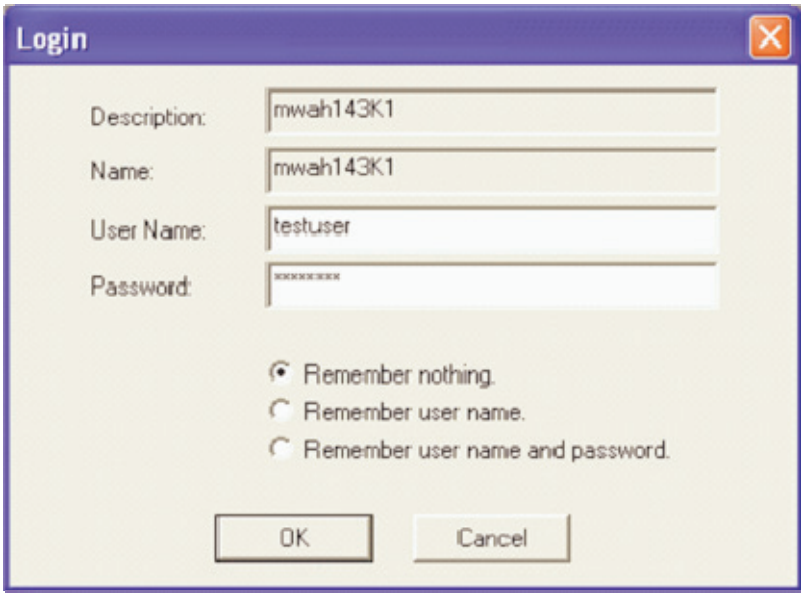


19. An Updating Other Page dialog appears. Click OK to continue.



20. When the Properties window appears, click Close.

21. In MPC or RRC, connect to the Dominion device by double-clicking on its icon in the Navigtor and perform tasks as allowed by the user group you specified.



Appendix C FAQs

In This Chapter

General Questions

Question	Answer
What is the Dominion KX?	The Dominion KX is a digital KVM (keyboard/video/mouse) switch that enables IT administrators to access and control 16 or 32 servers over the network with BIOS-level functionality. The Dominion KX is completely hardware and OS-independent; users can troubleshoot and reconfigure servers even when servers are down. At the rack, the Dominion KX provides the same functionality, convenience, space savings, and cost savings as do traditional analog KVM switches. However, the Dominion KX also integrates the industry's highest-performing KVM Over IP technology, thereby allowing multiple administrators to access server KVM consoles from any networked workstation in the world.

Question	Answer
How does the Dominion KX differ from remote control software?	When using the Dominion KX remotely, the interface, at first glance, may seem similar to remote control software such as PC Anywhere, Windows Terminal Services/Remote Desktop, VNC, etc. However, because the Dominion KX is not a software but a hardware solution, it is much more powerful: OS and hardware independent - The Dominion KX can be used to manage any type of server running any OS, whether Intel, Sun, PowerPC running Windows, Linux, Solaris, Novell, etc. State-independent/Agent-less - The Dominion KX does not require the managed server OS to be up and running, nor does it require any special software to be installed on the managed server. Out-of-Band - Even if the managed server's own network connection is unavailable, it can still be managed through the Dominion KX. BIOS-level access - Even if the server is hung at boot up, requires booting to safe mode, or requires system BIOS parameters to be altered, the Dominion KX still works flawlessly to enable these configurations to be made.
Can the Dominion KX be rack mounted?	Yes, the Dominion KX ships standard with 19" rack mount brackets. It can also be reverse rack mounted such that the server ports face forward.
How large is the Dominion KX?	The Dominion KX is only 1U in height, fits in a standard 19" rack mount, and occupies only 11.4" (29 cm) in depth. The Dominion KX464, supporting 64 server ports, however is a 2U device.

Remote Access

Question	Answer
How many users can remotely access servers on each Dominion KX?	Currently, Dominion models KX416, KX432, and KX464 offer concurrent remote transmissions of up to four unique servers at any time. The Dominion KX can, thereby, provide any of the following permutations: • 1 User, viewing four unique servers simultaneously • 2 Users, each viewing two unique servers simultaneously • 8 Users - eight users viewing one server; four users each viewing two unique servers simultaneously • Any other permutations of up to 8 users, viewing up to 4 unique servers total.

Question	Answer
Can two people look at the same server at the same time?	Yes, up to eight people can look at the same server at the same time.
Can two people access the same server, one remotely and one from the Local Console?	Yes, the Local Console is completely independent of the remote "ports." The Local Console can access the same server using the PC Share feature.
In order to access the Dominion KX from a client, what hardware, software, or network configuration is required?	Because the Dominion KX is completely web-accessible; it does not require proprietary software to be installed on clients used for access. (Although an optional installed client is available on the Raritan web site (*www.raritan.com* (http://www.raritan.com)) for the purposes of accessing the Dominion KX via modem). The Dominion KX can be accessed through major web browsers including: Internet Explorer, Netscape, Mozilla, and Firefox. The Dominion KX can now be accessed on Windows, Linux, SUN Solaris, and Macintosh desktops, with the introduction of Raritan's Java-based Multi Platform Client (MPC). The Dominion KX administrators can also perform remote management (set passwords and security, rename servers, change IP address, etc.). To perform remote management from a given workstation, you must also have Java Runtime Environment of v1.4.2.05 or later installed.

<table>
<tr><th>Question</th><th>Answer</th></tr>
<tr><td>What is the file size of the applet used to access the Dominion KX? How long does it take to retrieve?</td><td>The applet used to access the Dominion KX is approximately 1.4MB in size. The following chart describes the time required to retrieve the Dominion KX's applet at different network speeds:
<table>
<tr><td>100Mbps</td><td>Theoretical 100Mbit network speed</td><td>0.1 seconds</td></tr>
<tr><td>60Mbps</td><td>Likely practical 100Mbit network speed</td><td>0.2 seconds</td></tr>
<tr><td>10Mbps</td><td>Theoretical 10Mbit network speed</td><td>1.1 seconds</td></tr>
<tr><td>6Mbps</td><td>Likely practical 10Mbit network speed</td><td>2 seconds</td></tr>
<tr><td>512Kbps</td><td>Cable modem download speed (typical)</td><td>22 seconds</td></tr>
<tr><td>56Kbps</td><td>Dial-up modem theoretical speed</td><td>3 minutes</td></tr>
<tr><td>38Kbps</td><td>Likely practical dial-up modem speed</td><td>5 minutes</td></tr>
</table></td></tr>
<tr><td>How do I access servers connected to the Dominion KX if the network ever becomes unavailable?</td><td>The Dominion KX offers a dedicated modem port for attaching an external modem. With this dedicated modem, your servers can still be remotely accessed in the event of a network emergency. Furthermore, the Dominion KX's Local Consoles always allow access to your servers from the rack, no matter the network condition.</td></tr>
<tr><td>Can non-Windows users use RRC?</td><td>Yes, using Raritan MPC, non-Windows users can connect to target servers through the Dominion KX. MPC can be run via web browsers and standalone. Refer to Raritan's MPC User Guide for more information.</td></tr>
<tr><td>My connection dropped and I got the error message “There was an unexpected communications error - connection terminated” - what should I do?</td><td>This might happen based the frequency with which you try to connect via modem. Reboot the KX unit and modem, and for future connections, wait at least two (2) minutes between attempts.</td></tr>
</table>

Question	Answer
I am receiving a message that “All Video Channels are Busy (0x20001014)”. What does that mean?	The Dominion KX supports a certain number of simultaneous remote viewing sessions. If you are receiving this message, that number has been exceeded.

Ethernet and IP Networking

Question	Answer
How much bandwidth does the Dominion KX require?	The Dominion KX offers integrated IP-Reach technology - the very best video compression available. Raritan has received numerous technical awards confirming its high video quality transmissions and the low bandwidth utilization. Raritan pioneered the KVM Over IP functionality that allows users to tailor their video parameters to conserve network bandwidth. For instance, when connecting to the Dominion KX through a dial-up modem connection, video transmissions can be scaled to grayscale - allowing you to be fully productive while ensuring high performance. With that in mind, the following data refers to the Dominion KX at its default video settings - again, these settings can be tailored to your environment. They can be increased to provide even higher quality video (color depth), or decreased to optimize for low-speed connections. As a general rule, a conservative estimate for bandwidth utilization (at the Dominion KX's default settings) is approximately 0.5Mbit/seconds per active KVM user (connected to and using a server), with very occasional spikes up to 2MBit/seconds. This is a very conservative estimate because bandwidth utilization will typically be even lower. Bandwidth required by each video transmission depends on what task is being performed on the managed server. The more the screen changes, the more bandwidth is utilized. The following list summarizes some use cases and the required bandwidth utilization at the Dominion KX's default settings on a 10Mbit/s network: • Idle Windows Desktop - 0 Mbps • Move Cursor Around Desktop - 0.18Mbps • Move Static 400x600 Window/Dialog Box - 0.35Mbps • Navigate Start Menu - 0.49Mbps • Scroll an Entire Page of Text - 1.23Mbps • Run 3D Maze Screensaver - 1.55Mbps

Question	Answer
What is the slowest connection (lowest bandwidth) over which the Dominion KX can operate?	33Kbps or above is recommended for acceptable KX performance over a modem connection.
What is the speed of the Dominion KX's Ethernet interfaces?	The Dominion KX offers two 10/100 speed Ethernet interfaces, with configurable speed and duplex settings (either autodetected or manually set). The Dominion KX does not require a gigabit Ethernet interface because its output (see the previous question) would never even come close to exceeding the 100Mbit/sec limit of 10/100 Ethernet networking.
Can I access the Dominion KX over a wireless connection?	Yes. The Dominion KX not only utilizes standard Ethernet, but also uses very conservative bandwidth with very high quality video. Thus, if you have a wireless client with network connectivity to the Dominion KX, you can configure and manage your servers at BIOS-level wirelessly.
Can the Dominion KX used over the WAN (Internet), or just over the corporate LAN?	Yes. Whether via a fast corporate LAN, the less predictable WAN (Internet), a cable modem, or dial-up modem, the Dominion KX's KVM Over IP technology can accommodate your connection. Raritan's IP-Reach KVM Over IP technology is integrated into every Dominion KX unit. Raritan pioneered configurable video compression technology, leading the industry by years, as evidenced by its awards.
Can I use the Dominion KX with a VPN?	Yes. The Dominion KX uses standard Internet Protocol (IP) technologies from Layer 1 through Layer 4. Traffic can be easily tunneled through any standard VPN.
How many TCP ports must be open on my firewall in order to enable network access to the Dominion KX? Are these ports configurable?	Only one. The Dominion KX protects your network security by only requiring access to a single TCP port to operate. This port is completely configurable for additional security. To utilize the Dominion KX's optional web browser capability, the standard HTTPS port 443 must also be open.
Does the secondary network port provide redundant fail-over, or load balancing?	The secondary network port provides redundant fail-over capabilities: should the primary Ethernet port (or the switch/router to which it is connected) fail, the Dominion KX will fail-over to the secondary network port with the same IP address - ensuring that your server operations are not disrupted. Note that Automatic Failover is disabled by default.

Question	Answer
Does the Dominion KX require an external authentication server to operate?	No. The Dominion KX is a completely self-sufficient device. After assigning an IP address to the Dominion KX, it is ready to use - with web browser and authentication capabilities completely built-in. Of course, should you desire to use an external authentication server (such as LDAP, Active Directory, RADIUS, etc.), the Dominion KX allows you to, and will even fail-over to its own internal authentication should your external authentication server become unavailable. In this way, the Dominion KX's design philosophy is optimized to provide ease of installation, complete independence from any external server, and maximum flexibility.
Can the Dominion KX be used with CITRIX?	The Dominion KX may work with remote access products like CITRIX if configures appropriately, but Raritan cannot guarantee it will work with acceptable performance. Customers should realize that products like CITRIX utilize video redirection technologies similar in concept to digital KVM switches so that two KVM over IP technologies are being used simultaneously.
Can the Dominion KX utilize DHCP?	DHCP addressing can be used, however, Raritan recommends fixed addressing since the DKX is an infrastructure device and can be accessed and administered more effectively with a fixed IP address.
I'm having problems connecting to the Dominion KX over my IP network. What could be the problem?	The Dominion KX relies on the customer's LAN/WAN network. Some possible problems include: 1) Ethernet AutoNegotiation. On some networks 10/100 autonegotiation does not work properly and the KX unit must be set to 100MB/full duplex or the appropriate choice for its network. 2) Duplicate IP Address. If the IP Address of the KX is the same as another device, network connectivity may be inconsistent. 3) Port 5000 conflicts. If another device is using port 5000, the KX default port must be changed (or the other device must be changed). 4) When changing the IP Address of a KX or swapping in a new KX, sufficient time must be allowed for the KX IP and MAC Addresses to be known throughout the Layer 2 and Layer 3 networks.

Servers

Question	Answer
Does the Dominion KX depend on a Windows server to operate?	Absolutely not. Because you depend on your KVM infrastructure to always be available in any scenario whatsoever (as you will likely need to use your KVM infrastructure to fix problems), the Dominion KX is designed to be completely independent from any external server. For example, should your data center come under attack from a malicious Windows worm or virus, you will need to use your KVM solution to resolve the situation. Therefore, it is imperative that your KVM solution, in turn, must not rely on these same Windows servers (or any server, for that matter) to be operational in order for the KVM solution to function. To this end, the Dominion KX is completely independent. Even if you choose to configure your Dominion KX to authenticate against an Active Directory server - if that Active Directory server becomes unavailable, the Dominion KX's own authentication will be activated and fully functional.
Do I need to install a web server such as Microsoft Internet Information Services (IIS) in order to utilize the Dominion KX's web browser capability?	No. The Dominion KX is a completely self-sufficient device. After assigning an IP address to the Dominion KX, it is ready to use - with web browser and authentication capabilities completely built-in.
What software do I have to install in order to access the Dominion KX from a particular workstation?	None. The Dominion KX can be accessed completely via a web browser. (Although an optional installed client is provided on Raritan's web site (***www.raritan.com*** (http://www.raritan.com)) for the purpose of accessing the Dominion KX via modem.) A Java-based client is now available for non-Windows users.
What should I do to prepare a server for connection to the Dominion KX?	Servers connected to the Dominion KX do not require any software agents to be installed, because the Dominion KX connects directly via hardware to servers' keyboard, video, and mouse ports. In order to provide users with the best mouse synchronization during remote connections.

Question	Answer
What comes in the Dominion KX box?	(a) The Dominion KX unit; (b) quick setup guide; (c) standard 19" rack mount brackets; (d) User manual CD-ROM; (e) Network cable; (f) Crossover cable; (g) Localized AC Line Cord; (h) Warrantee certificate and other documentation.

Installation

Question	Answer
Besides the unit itself, what do I need to order from Raritan to install the Dominion KX?	For each server that you wish to connect to the Dominion KX, you will require a Dominion computer interface module (DCIM), a very small dongle that connects directly to the keyboard, video, and mouse ports of your server.
What kind of Cat5 cabling should be used in my installation?	The Dominion KX can use any standard UTP (twisted pair) cabling, whether Cat5, Cat5e, or Cat6. Often in our manuals and marketing literature, Raritan will simply say “Cat5” cabling for short. In actuality, any brand UTP cable will suffice for the Dominion KX.
What types of servers can be connected to the Dominion KX?	The Dominion KX is completely vendor independent. Any server with a standards-compliant keyboard, video, and mouse ports can be connected.
How do I connect servers to the Dominion KX?	For each server that you wish to connect to the Dominion KX, you will require a Dominion computer interface module (DCIM), a very small dongle that connects directly to the keyboard, video, and mouse ports of your server. Then, connect each dongle to the Dominion KX using standard UTP (twisted pair) cable such as Cat5, Cat5e, or Cat6.
How far can my servers be from the Dominion KX?	Servers can be up to 150 feet (45 m) away from the Dominion KX (see table in ***Appendix A: Specifications*** (see "Specifications" on page 217) for additional information).

Question	Answer
Some operating systems "lock up" if you disconnect a keyboard or mouse during operation. What prevents servers connected to the Dominion KX from "locking up" when users switch away from them?	Each Dominion computer interface module (DCIM) dongle acts as a virtual keyboard and mouse to the server to which it is connected. This technology is called KME (keyboard/mouse emulation). Raritan's KME technology is data center grade, battle-tested, and far more reliable than that found in lower end KVM switches: it incorporates more than 15-years of experience, has been deployed to millions of servers worldwide.
Are there any agents that must be installed on servers connected to the Dominion KX?	Servers connected to the Dominion KX do not require any software agents to be installed, because the Dominion KX connects directly via hardware to servers' keyboard, video, and mouse ports.
How many servers can be connected to each Dominion KX unit?	The Dominion KX models range, offering up to 32 server ports per 1U sized unit and 64 server ports in a 2U sized unit; this is the industry's highest digital KVM switch port density.
What happens if I disconnect a server from the Dominion KX and reconnect it to another Dominion KX unit, or connect it to a different port on the same Dominion KX unit?	The Dominion KX will automatically update the server port names when servers are moved from port to port. Furthermore, this automatic update does not just affect the local access port, but it propagates to all remote clients and the optional CC-SG management device.
How do I connect a serially controlled (RS-232) device to the Dominion KX, such as a Cisco router/switch or a headless Sun server?	If you only have a few serially-controlled devices, you may connect them to the Dominion KX using Raritan's serial computer interface module (CIM), Raritan AUATC. However, if you have four or more serially controlled devices, we recommend the use of Raritan's Dominion SX model line of secure console servers. For multiple serial devices, Dominion SX offers more functionality at a better price point than the Dominion KX, while being just as easy to use, configure and manage, and can be completely integrated with your Dominion Series deployment. In particular, many UNIX and networking administrators appreciate the ability to directly SSH to a Dominion SX unit (which the Dominion KX, a digital KVM switch, does not offer).

Local Console

Question	Answer
Can I access my servers directly from the rack?	Yes, at the rack the Dominion KX functions just like a traditional KVM switch - allowing you to control up to 64 servers using a single keyboard, mouse, and monitor.
When I am using the Local Console, do I prevent other users from accessing servers remotely?	No. The Dominion KX Local Console has a completely independent access path to the servers. This means a user can access servers locally at the rack - without compromising the number of users that access the rack remotely at the same time.
Can I use a USB keyboard or mouse at the Local Console?	Yes. The Dominion KX offers both PS/2 and USB keyboard and mouse ports on the local rack. Note that the USB ports are USB v1.1, and support keyboards and mice only - not USB devices such as scanners or printers. The Dominion KX supports select keyboard drawers, USB combo devices, PS2 to USB adapters and USB, hub-connected mice, keyboards, and/or hubs (1.4.7 and above).
How do I select between servers while using the Local Console? Is there an On-Screen Display (Locale Console)?	Yes. The Dominion KX's local access port displays an onscreen display interface that presents a list of all servers connected to the Dominion KX unit. Users interact with this convenient onscreen display interface to select a connected server.
How do I ensure that only authorized users can access servers from the Local Console?	The Dominion KX offers the very best Local Console authentication scheme available on the market: users attempting to use the Local Console must pass the same level of authentication as those accessing remotely. This means that: If you have configured the Dominion KX to interact with an external RADIUS, LDAP, or Active Directory server, users attempting to access the Local Console will authenticate against the same server. If the external authentication servers are unavailable, the Dominion KX fails-over to its own internal authentication database. The Dominion KX has its own standalone authentication, enabling instant on out-of-the-box installation. Note: this function is applicable when the Disable Login Menu option is set to No.

Question	Answer
If I use the Local Console to change the name of a connect server, does this change propagate to remote access clients as well? Does it propagate to the optional CC-SG device?	Yes. The Local Console presentation is identical and completely in sync with remote access clients, as well as Raritan's optional CC-SG management device. To be clear, if you change the name of a server via the Dominion KX onscreen display, this updates all remote clients and external management servers in real-time.
If I use the Dominion KX's remote administration tools to change the name of a connected server, does that change propagate to the Local Console Locale Console as well?	Yes, if you change the name of a server remotely, or via Raritan's optional CC-SG management device, this update immediately affects the Dominion KX's onscreen display.

Power Control

Question	Answer
What type of power control capabilities does the Dominion KX offer?	Because the Dominion KX enables you to remotely manage servers; it also incorporates the critical functionality of hard power control to servers. Instead of using a third-party tool for power control (likely with lower security and fail-safe capabilities as the Dominion KX), you can use the Dominion KX's fully integrated remote power control. When remotely connected to an appropriately configured the Dominion KX, simply select the power control options to hard reboot a hung server. Note that a hard reboot provides the physical equivalent of unplugging the server from the AC power line, and re-inserting the plug.
Does the Dominion KX support servers with multiple power supplies? What if each power supply is connected to a different power strip?	Yes. The Dominion KX can be easily configured to support multiple power supplies connected to multiple power strips. Up to eight (8) powerstrips can be connected to a KX device. Four power supplies can be connected per target server to multiple power strips.

Question	Answer
Does remote power control require any special server configuration?	Some servers ship with default BIOS settings such that the server does not restart after losing and regaining power. See your server user guide for more details.
What type of power strips does the Dominion KX support?	The Dominion KX can support any serially controlled power strips supplied by any vendor, by using our Serial (RS-232) computer interface module. However, to take advantage of the Dominion KX's integrated power control user interface, and more importantly, integrated security, you must use Raritan's power strips (“remote power control units”). These power strips come in many outlet, connector, and amp variations - simply order any Raritan power strip whose part number ends in the “-PK” designation.

Computer Interface Modules (CIMs)

Question	Answer
Can I use Computer Interface Modules (CIMs) from Raritan's analog matrix KVM switch, Paragon, with the Dominion KX?	Yes. Certain Paragon computer interface modules (CIMs) may work with the Dominion KX (please check the Raritan web site for the latest list of certified CIMs). However, because Paragon CIMs cost more than the Dominion KX CIMs (as they incorporate technology for video transmission of up to 1000 feet [300 meters]), it is not generally advisable to purchase Paragon CIMs for use with the Dominion KX. Also note that when connected to the Dominion KX, Paragon CIMs transmit video at a distance of 50 feet [15 meters], the same as the Dominion KX CIMs - not at 1000 feet [300 meters], as they do when connected to Paragon.
Can I use Z-Series “daisy-chaining” Computer Interface Modules (CIMs) with the Dominion KX?	At the present time, Raritan's Z-Series “daisy-chaining” computer interface modules do not work with the Dominion KX. This capability will be incorporated in future releases - requiring only a firmware upgrade.

Question	Answer
Can I use the Dominion KX Computer Interface Modules (CIMs) with Raritan's analog matrix KVM switch, Paragon?	No. Dominion KX computer interface modules (CIMs) transmit video at ranges of 50 to 150 feet (15 - 45 m) and thus do not work with Paragon, which requires CIMs that transmit video at a range of 1000 feet (300 meters). To ensure that all Raritan's customers experience the very best quality video available in the industry - a consistent Raritan characteristic - Dominion Series CIMs do not interoperate with Paragon.

Scalability

Question	Answer
How do I connect multiple Dominion KX devices together into one solution?	Multiple Dominion KX units do not need to be physically connected together. Instead, each Dominion KX unit connects to the network, and they automatically work together as a single solution: If you deploy Raritan's optional CC-SG management device, CC-SG acts as a single access point for remote access and management. CC-SG offers a significant set of convenient tools, such as consolidated configuration, consolidated firmware update, and a single authentication and authorization database. In addition, CC-SG enables sophisticated server sorting, permissions, and access functionality - for instance, you can create an attribute called “Operating System”, and in one step enable only the Active Directory group “SYSADMINS” to access those servers whose “Operating System” attribute is set to “Windows.” Refer to the CC-SG FAQ sheet on Raritan's web site (www.raritan.com). If you do not take advantage of Raritan's optional CC-SG management device, multiple Dominion KX units still interoperate and scale automatically: The Raritan Remote Client automatically discovers the Dominion KX units in your subnet. You can access Dominion KX units outside the subnet via a user-created profile.

Question	Answer
Can I connect an existing analog KVM switch to the Dominion KX?	Yes. You can connect your analog KVM switch to one of the Dominion KX's server ports. Simply use a PS/2 Computer Interface Module (CIM), and attach it to the user ports of your existing analog KVM switch. Note that analog KVM switches vary in their specifications and Raritan cannot guarantee the interoperability of any particular third-party analog KVM switch. Contact Raritan technical support for further information. Raritan's Paragon and Paragon II analog switches are IP enabled by the IP-Reach family of remote access products.

Security

Question	Answer
What kind of encryption does the Dominion KX use?	The Dominion KX utilizes industry-standard (and extremely secure) 128-bit RC4 encryption, both in its SSL communications as well as its own data stream. Literally no data is transmitted between remote clients and the Dominion KX that is not completely secured by encryption.
Does the Dominion KX allow encryption of video data? Or does it only encrypt keyboard and mouse data?	Unlike competing solutions, which only encrypt keyboard and mouse data, the Dominion KX does not compromise your security - it allows encryption of keyboard, mouse and video data.
How does the Dominion KX integrate with external authentication servers such as Active Directory, RADIUS, or LDAP?	Through a very simple configuration, the Dominion KX can be set to forward all authentication requests to an external server such as LDAP, Active Directory, or RADIUS. For each authenticated user, the Dominion KX receives from the authentication server the user group to which that user belongs. Dominion KX then determines the user's access permissions depending on what user group to which he belongs.
How are usernames and passwords stored?	Should you use the Dominion KX's internal authentication capabilities, all sensitive information such as usernames and passwords are stored in a hashed format. Literally no one, including Raritan technical support or Product Engineering departments, can retrieve those usernames and passwords.

Manageability

Question	Answer
Can the Dominion KX be remotely managed and configured via web browser?	Yes. The Dominion KX can be completely configured remotely via web browser. Note that this does require that your workstation have Java Runtime Environment 1.4.2 installed. Besides the initial setting of the Dominion KX's IP address, everything about the solution can be completely set up over the network. (In fact, using a crossover Ethernet cable and the Dominion KX's default IP address, you can even configure even the initial settings configured via web browser.)
Can I backup and restore the Dominion KX's configuration?	Yes, the Dominion KX's device and user configurations can be completely backed up for later restoration in the event of a catastrophe. More commonly, this functionality is also very useful for configuring multiple Dominion KX units if you have not deployed Raritan's CC-SG centralized management device. You can back up the user configuration and restore it on remaining units. The Dominion KX's backup and restore functionality can be utilized remotely over the network; in fact, via a web browser.
What auditing or logging does the Dominion KX offer?	For complete accountability, the Dominion KX logs all major user events with a date and time stamp. For instance, reported events include (but are not limited to): user login, user logout, user access of a particular server, unsuccessful login, configuration changes, etc
Can the Dominion KX integrate with syslog?	Yes, for your convenience, in addition to the Dominion KX's own internal logging capabilities, the Dominion KX can also send the following logged events to a centralized syslog server: Network Admin Error Text System
Can the Dominion KX's internal clock be synchronized with a timeserver?	Yes, the Dominion KX supports the industry-standard NTP protocol for synchronization with either your corporate timeserver, or with any public time server [assuming that outbound NTP requests are allowed through your corporate firewall].

Question	Answer
Does the power supply used by the Dominion KX automatically detect voltage settings?	Yes, the Dominion KX's power supply can be used in any AC voltage ranges from 100-240 volts, at 50-60 Hz.

Miscellaneous

Question	Answer
What is Dominion KX's default IP address?	192.168.0.192
What is Dominion KX's default user name and password?	For the highest level of security, Raritan highly recommends that users reconfigure their Dominion KX default administrative user name and password of (admin/raritan [all lower case]) as soon as the unit is connected to the network.
I changed and subsequently forgot the Dominion KX's administrative password; can you retrieve it for me?	KX Release 1.3 contains a local reset feature that can be used to factory reset the device, which will reset the administrative password on the device. Alternately, the KX can be configured to reset the administrative password.
Is 24/7 Technical Support available for the Dominion KX?	Yes, Raritan offers an extended warranty that that provides 24/7 support; contact Raritan for additional information. During office hours, contact your local Raritan Technical Support office. See the cover of this guide for support contact information.

Index

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Raritan.
When you're ready to take control®

➢ *U.S./Canada/Latin America*

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

➢ *China*

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

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

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

➢ *India*

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

➢ *Japan*

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

➢ *Europe*

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

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

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

➢ *Korea*

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

➢ *Melbourne, Australia*

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

➢ *Taiwan*

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