Dominion KSX

User Manual

DKSX440

DKSX880

Raritan.

This page intentionally left blank.

Dominion KSX

User Manual

DKSX440
DKSX880

LISTED 1F61 I.T.E.

KSX-0A-E
August 2003
255-80-5020

Raritan Computer Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tel. 1-732-764-8886
Fax. 1-732-764-8887
sales@raritan.com
http://www.raritan.com

Raritan Computer Europe, B.V.
Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
Tel. 31-10-284-4040
Fax. 31-10-284-4049
sales.europe@raritan.com
http://www.raritan.com

Raritan Computer Japan, Inc.
Kuga Building 7F
11-6, Kuramae 4-chome
Taitoo-ku, Tokyo 111-0051, Japan
Tel. 81-3-5833-6360
Fax. 81-3-5833-6336
sales.japan@raritan.com
http://www.raritan.co.jp

Raritan Computer Taiwan, In
5F, 121, Lane 235,
Pao-Chiao Rd., Hsin Tien
Taipei Hsien, Taiwan, ROC
Tel. 886-2-8919-1333
Fax. 886-2-8919-1338
sales.asia@raritan.com
http://www.raritan.com.tw

This page intentionally left blank.

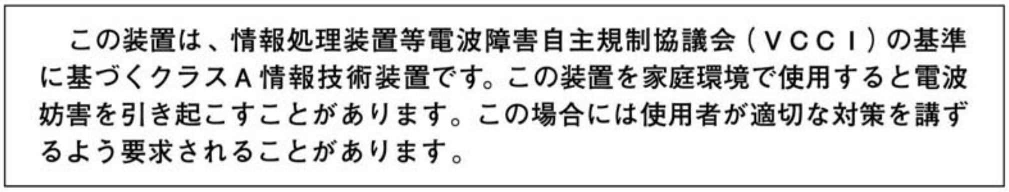
FCC Information

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

Trademark Information

Product names mentioned in this document are trademarks or registered trademarks of their respective companies. Dominion, IP-Reach, Paragon, MasterConsole MX^4, MasterConsole II, MasterConsole, and their respective logos are trademarks or registered trademarks of Raritan Computer, Inc. PS/2, RS/6000, and PC/AT are registered trademarks of International Business Machines Corporation. Sun is a registered trademark of Sun Microsystems. Microsoft and Windows are registered trademarks of Microsoft Corporation. All other marks are the property of their respective owners.

Japanese Approvals



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。

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

Important Information

Login

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

Default IP Address

- Dominion KSX ships with the default IP address of 192.168.0.192.

Firmware

- This manual applies to Dominion KSX Firmware v3.10 and above.

This page intentionally left blank.

Chapter 1: Introduction

Dominion KSX Overview

Congratulations on your purchase of Dominion KSX, the complete solution for remote office administration.

Dominion KSX is the first hardware based, integrated solution to provide remote KVM access, serial device management and power control in a single unit. With Dominion KSX, administrators may troubleshoot and control remote office server closets as if physically present at the branch office. Unlike remote control software solutions, Dominion KSX provides:

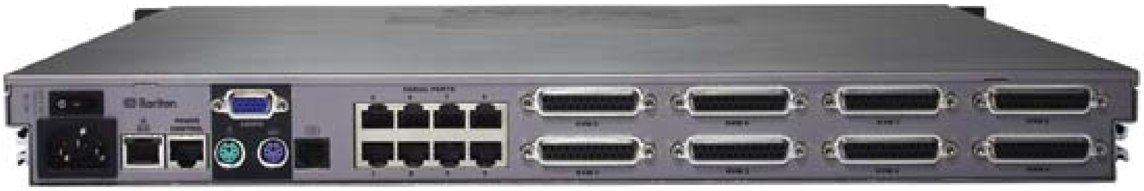
- One consolidated view of all IT equipment deployed at branch office locations
- A single, platform-independent solution offering centralized, integrated and secure control
- Network independent access via built-in modem for emergency access even when the network is down
- BIOS-level control of KVM equipment and console level control of serial devices

Raritan's Dominion KSX is designed specifically to make the management of your IT infrastructure at branch locations easier, faster and more cost-effective. This innovative device combines secure console level access and cold start power control of everything in your server closets. This means from anywhere you access the Web, you can directly access, troubleshoot and even reboot all of your remote equipment including:

- Domain Servers
- File/Print Servers
- Headless Servers
- Network Appliances
- Serial IT Equipment
- Switches
- Routers
- Firewalls
- Security Interfaces
- Application Servers
- Load Balancers
- Environmental Control

Product Photos

Dominion KSX Stacked View



Dominion KSX Rear View

Product Features

Access

- Remote access via the Internet, LAN/WAN, or dial-up modem
- Single integrated solution for remote serial console and KVM console access
- Web browser accessible
- Integrated, graphical remote power control interface
- Integrated modem allows remote office devices to be accessible even if network is unavailable
- Remote access to 4 or 8 KVM ports
- Remote access to 4 or 8 serial console ports

Performance

- Superior compression algorithm for exceptional performance over low-bandwidth connections
- No impact on target server performance
- Automatic sensing of video resolution for optimum display
- High-performance mouse tracking and synchronization

Security

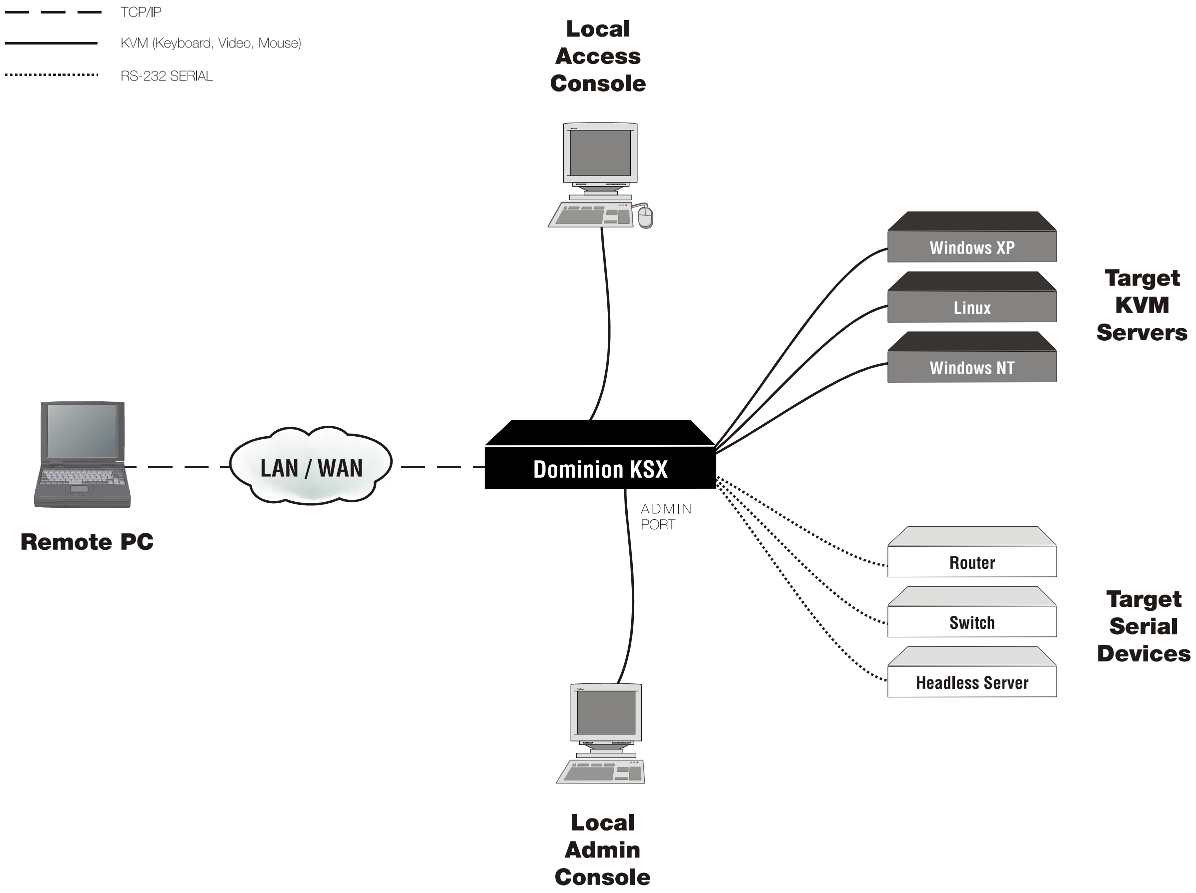
- SSL 128-bit RSA public key, 128-bit RC4 private key encryption
- Single, configurable TCP port for firewall protection
- Supports RADIUS authentication protocol
- Customizable user profiles

Administration

- Remote Administration via Web Browser interface
- SNMP Support
- Firmware upgradeable over Ethernet
- Simplified installation and user interface
- Local user console for direct analog access to KVM devices
- Extensive downloadable user event log
- DHCP or fixed IP addressing

Terminology

This manual makes use of the following terms to indicate components of a typical Dominion KSX configuration. While reading the manual, please refer to the diagram below for clarification when necessary.



Target KVM Servers Servers with graphical video cards and user interfaces (e.g., Windows, Linux, Solaris, etc.) to be accessed remotely via Dominion KSX.

Target Serial Devices Serially-controlled (RS-232) devices to be accessed remotely via Dominion KSX. For example, headless servers, routers, switches, CSU/DSU, etc.

Remote PC A networked Windows-based computer used to access and control target devices connected to Dominion KSX.

Local Access Console An **optional** user console, consisting of a PS/2 keyboard, PS/2 mouse, and multi-sync VGA monitor, directly attached to Dominion KSX to control Target KVM Servers locally (not through the network).

Local Admin Console A PS/2 keyboard and VGA monitor directly attached to Dominion KSX, used for administration and setup. From this console, Dominion KSX administration menus can be performed directly. Target KVM Servers and Target Serial Devices cannot be viewed using this screen.

While Dominion KSX also allows remote administration via the network, the local admin console provides the most convenient means to perform initial setup.

Package Contents

Dominion KSX ships as a fully configured stand-alone product in a standard 1U 19” rackmount chassis, along with the following contents:

(1) Dominion KSX unit

(1) Dominion KSX Quick Installation and Setup Guide

(1) Raritan User Manual CD-ROM

(1) Raritan Remote Client software CD-ROM

(1) Raritan Remote Client software license certificate for five named users

(1) Rackmount Kit

(1) AC Power Cord

(1) RJ11 telephone cord

(1) Cat5 Network cable

Chapter 2: Installation

Configuring Target KVM Servers

Before installing Dominion KSX, you must first configure any target KVM servers that you wish to access via Dominion KSX in order to ensure optimum performance, as outlined below. Note that the following configuration requirements apply only to *Target KVM Servers*, not to the computers that you will be using to access Dominion KSX remotely (see **Chapter 1: Introduction**, ***Terminology***).

Server Video Resolution

Ensure that each Target KVM Server's video resolution and refresh rate is supported by Dominion KSX, and the signal is non-interlaced. Dominion KSX supports the following video resolutions:

Text Modes
640x480 @ 60Hz
640x480 @ 72Hz
640x480 @ 75Hz
640x480 @ 85Hz
800x600 @ 56Hz
800x600 @ 60Hz
800x600 @ 72Hz
800x600 @ 75Hz
800x600 @ 85Hz
1024x768 @ 60Hz
1024x768 @ 70Hz
1024x768 @ 75Hz
1024x768 @ 85Hz
1152x864 @ 60Hz
1152x864 @ 75Hz
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.

Windows XP / Windows 2003 Settings

On target servers running Microsoft Windows XP, disable the "Enhanced Pointer Precision" option, and set the mouse motion speed exactly to the middle speed setting. These parameters are found in **Control Panel → Mouse → Mouse Pointers**.

Note: *For Target Servers running Windows NT, 2000, or XP, you may wish to create a username that is to be used only for remote connections through Dominion KSX. This will enable you to keep the Target Server's slow mouse pointer motion/acceleration settings exclusive to the Dominion KSX connection only, as other users may desire faster mouse speeds.*

Note: *Windows XP and 2000 login screens revert to pre-set mouse parameters that differ from those suggested for optimal Dominion KSX performance. As a result, mouse sync will not be optimal at these screens. If you are comfortable adjusting the registry on Windows target servers, you can obtain better Dominion KSX 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.*

Disable transition effects in **Control Panel → Display → Appearance → Settings**.

Windows 2000 / ME 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 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 Settings

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

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

To check for these parameters:

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

<u>Note:</u> *In many Linux graphical environments, the command <**Ctrl+Alt+Plus**> will change the video resolution, scrolling through all available resolutions that remain enabled in the XF86Config file.*

Sun Solaris Settings

As mentioned, all target servers must be configured to one of the display resolutions supported by Dominion KSX, as listed on page 6. The most popular supported resolutions for Sun machines are:

- 1024x768@60Hz
- 1024x768@70Hz
- 1024x768@75Hz
- 1024x768@85Hz
- 1152x900@66Hz
- 1152x900@76Hz
- 1280x1024@60Hz

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

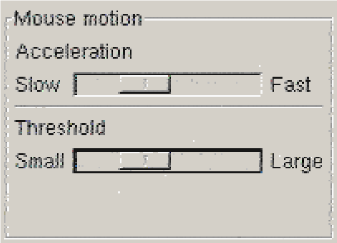
```
setenv output-device screen:r1024x768x70
```

to change the output resolution. Issue the “boot” command to reboot the server.

Alternatively, you may contact your Raritan representative to purchase a video output adapter. 13W3 Suns with composite sync output require APSSUN II Raritan guardian for use with Dominion KSX. HD15 Suns with composite sync output require 1396C Raritan converter to convert from HD15 to 13W3 and an APSSUN II Raritan guardian converter to support composite sync. HD15 Suns with separate sync output require an APKMSUN Raritan guardian for use with Dominion KSX.

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

This can be performed from the graphical user interface (as shown below), or with the command line “xset mouse a t” where “a” is the acceleration and “t” is the threshold.



Apple Macintosh Settings

For target servers running an Apple Macintosh operating system, while no specific mouse setting is required, please be aware that while using Dominion KSX to access and control your target server, you must set the Dominion KSX client (Raritan Remote Client) to “single cursor” mode (see **Chapter 3: Raritan Remote Client, *Remote KVM Console Control, Single Mouse Mode***).

Dual cursor mode is not supported; the two mouse pointers will not appear in sync if you attempt to control a Macintosh server via Dominion KSX in dual cursor mode.

Configuring Target Serial Devices

For each target serial device that you wish to connect to Dominion KSX for remote access, please:

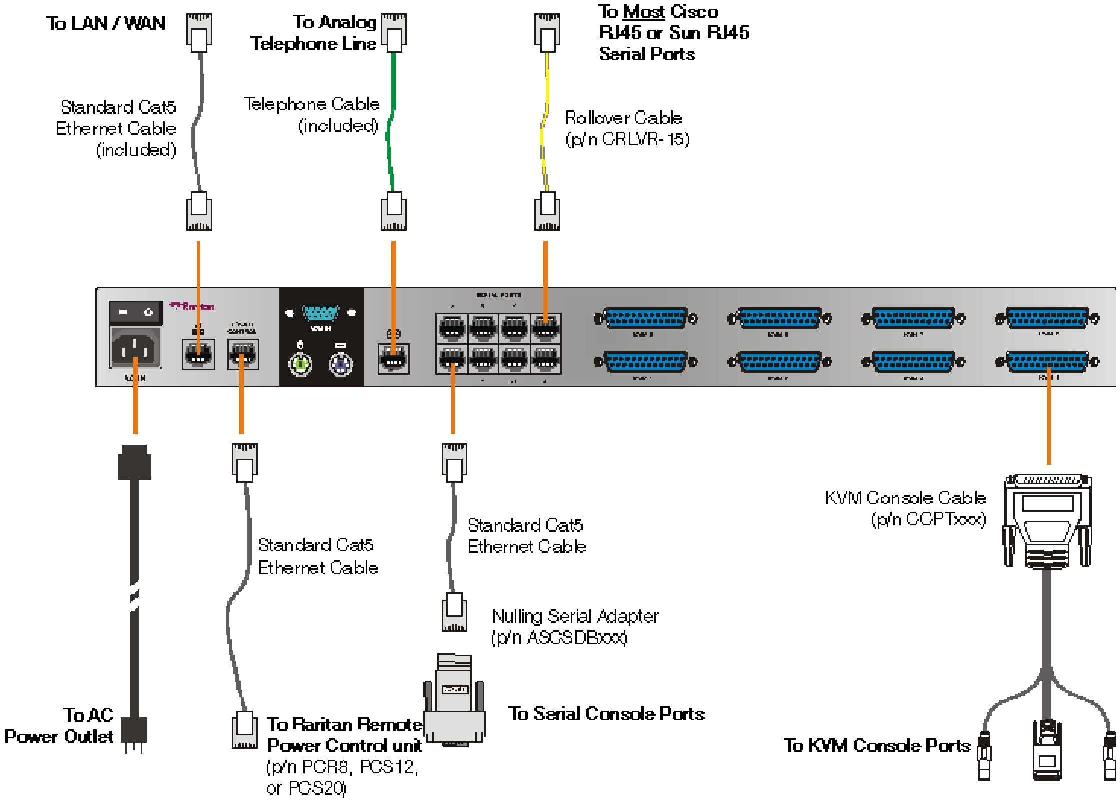
- Ensure that the serial terminal settings are set to a VT-100 emulation. Dominion KSX supports only standard VT-100 emulation.
- Either change the serial communication parameters to 9600 baud N-8-1 (Dominion KSX default), or note the communication parameters for later reference.

Configuring Network Firewall Settings

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

Optional: If you wish to take advantage of Dominion KSX's web-access capabilities, the firewall must also allow inbound communication on TCP Port 443 – the standard TCP port for HTTPS communication. If you wish to take advantage of Dominion KSX's automatic redirection of HTTP requests to HTTPS (i.e., so users may type the more common, "http://xxx.xxx.xxxx", instead of "https://xxx.xxx.xxxx"), then the firewall must also allow inbound communication on TCP Port 80 – the standard TCP port for HTTP communication.

Physical Connections


To LAN / WAN
Standard Cat5 Ethernet Cable (included)
To Analog Telephone Line
Telephone Cable (included)
To Most Cisco RJ45 or Sun RJ45 Serial Ports
Rollover Cable (p/n CRLVR-15)
To AC Power Outlet
Standard Cat5 Ethernet Cable
To Raritan Remote Power Control unit (p/n PCR8, PCS12, or PCS20)
Standard Cat5 Ethernet Cable
Nulling Serial Adapter (p/n ASCSDBxxx)
To Serial Console Ports
KVM Console Cable (p/n CCPTxxx)
To KVM Console Ports

Back Panel of Dominion KSX

AC Power Line

Attach the included AC power cord to Dominion KSX and into an AC Power Outlet.

Network Port

Connect a standard Ethernet cable from the network port to an Ethernet switch, hub, or router.

Power Control Port (optional)

To employ Dominion KSX's integrated power control graphical interface, connect a standard Cat5 Ethernet cable from the port labeled "Power Control" to the equivalently labeled port found on a Raritan Remote Power Control unit (p/n PCR8, PCS12, or PCS20).

***Note**: This port works only with Raritan brand Remote Power Control units. You may use similar products from other vendors by connecting them as a standard serial device. However, note that Dominion KSX does not present a graphical interface to other vendors' power control products, only a standard command-line interface; Dominion KSX's graphical power control interface applies only to Raritan brand Remote Power Control units.*

Local Admin Console

Attach a PS/2 keyboard and multisync monitor to the indicated ports (see diagram above) in the back of Dominion KSX. The local Admin Console is very useful during initial setup, and may be removed thereafter.

Telephone Line Port (optional)

Dominion KSX features an integrated modem for remote access even when the LAN/WAN is unavailable. Use the included telephone cable to connect the port labeled "Tel Line" to an analog telephone jack.

Serial Input Ports

Connect RS-232 serially-controlled devices to Dominion KSX for the ability to remotely access terminal console ports on devices such as headless servers, routers, switches, and network appliances. For each serial console port for which you wish to provide remote access via Dominion KSX, connect the serial interface to Dominion KSX as appropriate to the physical form factor of your serial console port:

- **DB9 Serial Ports:** Attach one end of a standard, straight-through Cat5 cable to an unoccupied RJ45 serial port on the back of your Dominion KSX. Attach the other end of the Cat5 cable to a Raritan nulling serial adapter: P/N ASCSDB9F for DB9 (M) serial ports; and P/N ASVSDB9M for DB9 (F) serial ports. Then, attach the Raritan nulling serial adapter directly to your device's serial console port.
- **DB25 Serial Ports:** Attach one end of a standard, straight-through Cat5 cable to an unoccupied RJ45 serial port on the back of your Dominion KSX. Attach the other end of the Cat5 cable to a Raritan nulling serial adapter: P/N ASCSDB25F for DB25 (M) serial ports; and P/N ASVSDB25M for DB25 (F) serial ports. Then, attach the Raritan nulling serial adapter directly to your device's serial console port.
- **RJ45 Serial Ports (from Sun and Cisco):** Most Sun and Cisco RJ45 Serial Ports may be connected directly to an unoccupied RJ45 serial port on the back of your Dominion KSX, using a "rollover" cable whose pin-outs are described in *Appendix B: Serial Port Pin-Out Diagrams*, "CRLVR-15 Custom Rollover Cable for Most Sun / Cisco RJ45 Serial Ports". This cable is often provided by Sun and Cisco in shipments of their products whose serial ports have the RJ45 form factor. Alternatively, this cable may be purchased directly from Raritan – order part number CRLVR-15.
- **RJ45 Serial Ports (from vendors other than Sun and Cisco):** Unfortunately, no widely accepted standard for RS-232 serial signal transmission through an RJ45 form factor port currently exists. Therefore, to connect an RJ45 serial port to Dominion KSX, refer to your vendor's product manual to obtain a pin-out diagram of its RJ45 serial console port. Then, using Cat5 cable with RJ45 terminators, crimp a cable in order whose pin-out corresponds correctly to Dominion KSX specifications as found in Appendix B of this manual.

  For your reference, the following chart can assist you in creating, modifying, or confirming such a custom cable:

Dominion KSX Serial Port Pin	Function	Proper Nulling Connection to Your Serial Console*	Port Pin of Your Serial Console**
1	RTS	CTS §	
2	DTR	DSR and DTD §	
3	TXD	RX ("RXD")	
4	GND	GND	
5	SGND	GND or SGND	
6	RXD	TX ("TXD")	
7	DSR	DTR §	
8	CTS	RTS §	

Notes:

* Standard serial nulling signal associations as specified by RS-232.

** Fill in this column with values specified by the device manual provided with your serially-controlled device.

§ In most cases, this signal is optional – generally used only if hardware flow control is enabled.

KVM Input Ports

To connect servers with graphical video cards, such as those running Microsoft Windows or Linux, attach the DB25 end of a Raritan KVM Console Cable (p/n CCPTxxx) to a KVM port found on the back panel of Dominion KSX. Connect the other end of the cable to corresponding PS/2 keyboard, mouse, and VGA video ports of the server to which you wish to provide remote network access.

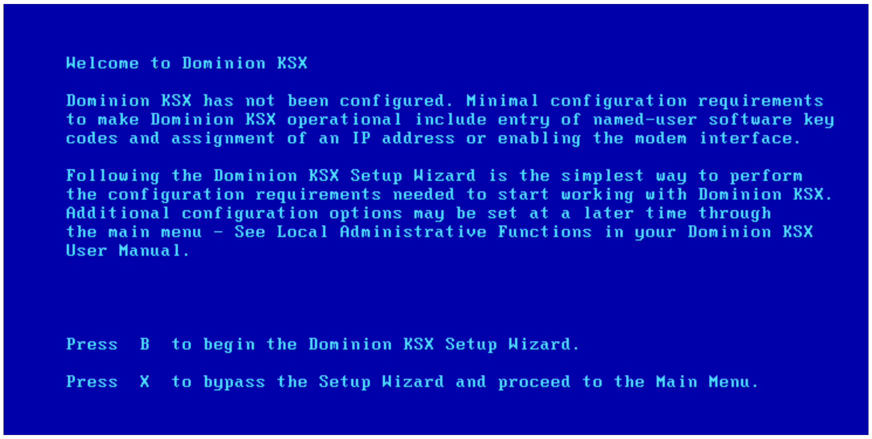
KVM Output / Local Access Console Ports (optional) (on front of chassis)

For convenient access to Target KVM Servers while onsite (in the presence of Dominion KSX), you may choose to take advantage of Dominion KSX's Local Access Console ports, located on the front of the chassis. To do so, first remove the front bezel by pulling it horizontally towards you. Then, attach a multisync VGA monitor, PS/2 mouse, and PS/2 keyboard to the ports located on the right hand side.

Initial Configuration

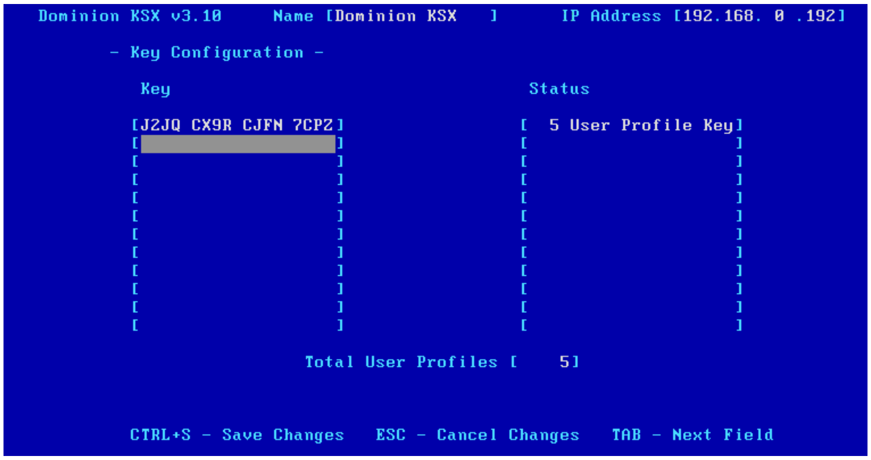
The steps below allow you to quickly set up Dominion KSX for the first time using the **Dominion KSX Setup Wizard**. The Dominion KSX Setup Wizard appears only when accessing the Administrative Menus on an unconfigured Dominion KSX, and guides you through initial configuration parameters. The easiest way to perform this initial configuration is by using the Local Admin Console (see 'Physical Connection' instructions in the previous sections).

1. Power ON Dominion KSX via the power switch on the back of the Dominion KSX unit.
2. The Welcome to Dominion KSX Setup Wizard Screen will appear on the Local Admin Console.



```
Welcome to Dominion KSX

Dominion KSX has not been configured. Minimal configuration requirements
to make Dominion KSX operational include entry of named-user software key
codes and assignment of an IP address or enabling the modem interface.

Following the Dominion KSX Setup Wizard is the simplest way to perform
the configuration requirements needed to start working with Dominion KSX.
Additional configuration options may be set at a later time through
the main menu - See Local Administrative Functions in your Dominion KSX
User Manual.



Press  B  to begin the Dominion KSX Setup Wizard.

Press  X  to bypass the Setup Wizard and proceed to the Main Menu.
```

3. Press the letter <**B**> on the Local Admin Console keyboard to begin the Dominion KSX Setup Wizard.
4. The Key Configuration Screen will appear.

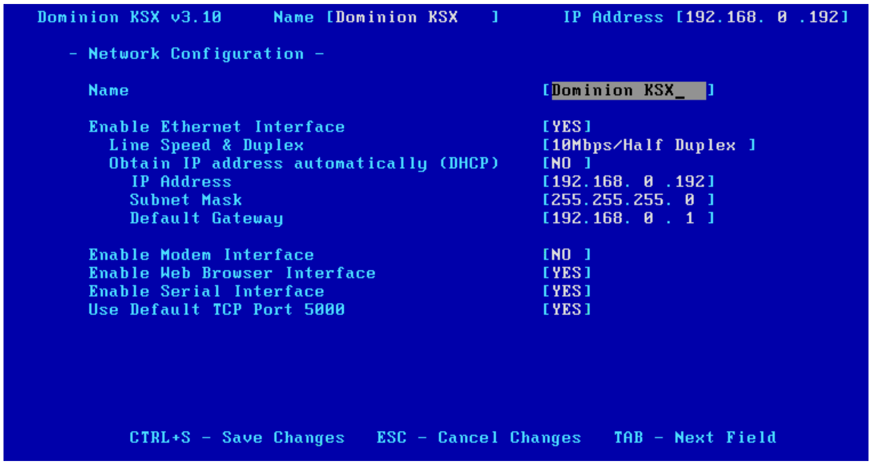


```
Dominion KSX v3.10     Name [Dominion KSX    ]      IP Address [192.168. 0 .192]

        - Key Configuration -

           Key                                  Status

          [J2JQ CX9R CJFN 7CPZ]                [  5 User Profile Key]
          [                   ]                [                    ]
          [                   ]                [                    ]
          [                   ]                [                    ]
          [                   ]                [                    ]
          [                   ]                [                    ]
          [                   ]                [                    ]
          [                   ]                [                    ]
          [                   ]                [                    ]
          [                   ]                [                    ]
          [                   ]                [                    ]
          [                   ]                [                    ]

                              Total User Profiles [    5]


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

On this screen, enter each Raritan Remote Client User License Key purchased, pressing <**Tab**> or <**Enter**> after each key is entered. Raritan Remote Client User License Key codes can be found on the license certificates shipped with your unit.

When all named-user keys are entered, press <**Ctrl+S**> to save the keys entered.

5. All entered key codes will be saved and the Network Configuration Screen will appear.



```
 Dominion KSX v3.10      Name [Dominion KSX    ]       IP Address [192.168.  0 .192]

    - Network Configuration -

      Name                                         [Dominion KSX_   ]

      Enable Ethernet Interface                    [YES]
        Line Speed & Duplex                        [10Mbps/Half Duplex ]
        Obtain IP address automatically (DHCP)     [NO ]
          IP Address                               [192.168.  0 .192]
          Subnet Mask                              [255.255.255.  0 ]
          Default Gateway                          [192.168.  0 .  1 ]

      Enable Modem Interface                       [NO ]
      Enable Web Browser Interface                 [YES]
      Enable Serial Interface                      [YES]
      Use Default TCP Port 5000                    [YES]



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

6. Use the <**Tab**>, <↑> or <↓> keys to select each line on the Network Configuration screen and the <**space bar**>, or the <←> or <→> keys to toggle between available entries. Press the <**Enter**>, <**Tab**> or <↓> keys when your entry on each line is complete. Below are descriptions of each field, and the appropriate values to assign.

- **Name**: Designate a unique name for this Dominion KSX unit, for example, "Miami Sales Office" The default name is **Dominion KSX**.
- **Enable Ethernet Interface**: Designates whether Dominion KSX should enable its Ethernet adapter as active (default: YES).

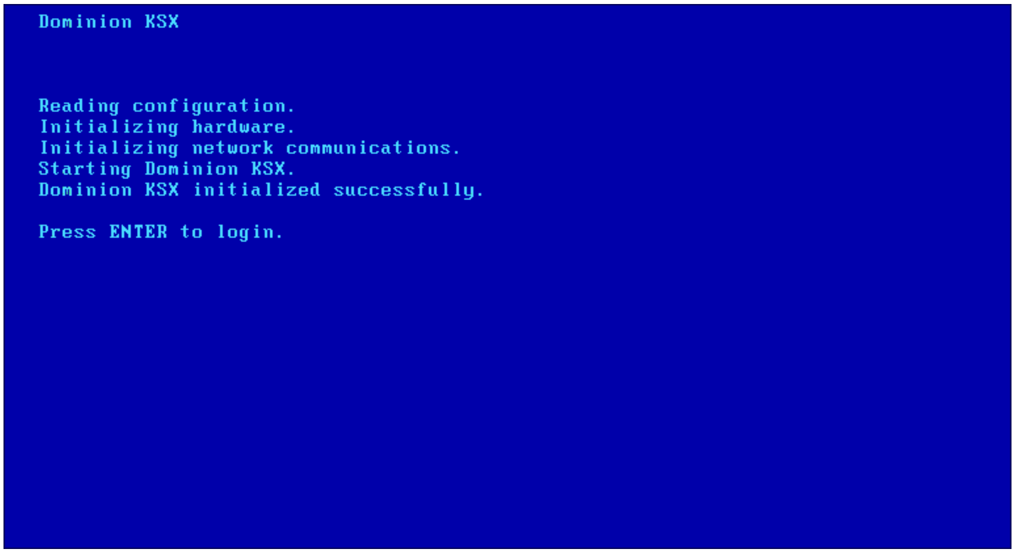
> ***Note***: *Network connections must be 10BASE-T or 100BASE-TX Ethernet*

  - **Line Speed & Duplex:** Enter the network speed to be used by Dominion KSX's Ethernet interface: Auto detect, 10 Mbps/Full Duplex, 10 Mbps/Half Duplex, 100 Mbps/Full Duplex, or 100 Mbps/Half Duplex
  - **Obtain IP address automatically (DHCP)**:
    - ♦ **YES:** Enables dynamic IP addressing for Dominion KSX. Each time Dominion KSX boots, it will request an IP address from the local DHCP server. Note that this setting can make remote access to Dominion KSX from outside the LAN difficult, since the dynamically assigned IP address must be known in order to initiate a connection.
    - ♦ **NO (default)**: Assigns a fixed IP address to the Dominion KSX unit (recommended).
      - ▪ **IP Address**: Enter the IP address for Dominion KSX given by your Network Administrator.
      - ▪ **Subnet Mask**: Enter a Subnet Mask provided by your Network Administrator.
      - ▪ **Default Gateway**: Enter the Default Gateway if your Network Administrator specifies one.

- **Enable Modem Interface**: Enables Dial-up Modem access (default: YES).
- **Enable Web Browser Interface**: Enables web browser access to Dominion KSX (default: YES).
- **Enable Serial Interface**: Enables remote access to the serial devices connected to Dominion KSX's Serial IN port (default: YES).
- **Use Default TCP Port 5000**:
  - **YES (default):** Utilizes the default port 5000.
  - **NO:** Enter an alternate port number.

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

7. Press <**Ctrl+S**> to save entries. The Main Menu will appear.
8. On the Main Menu, select **[R] Restart or shutdown the Dominion KSX**, and press the <**Enter**> key.
9. When prompted, press the letter <**R**> on your keyboard to restart Dominion KSX.
10. Dominion KSX will restart and the Dominion KSX Initialization screen will appear upon boot up.



```
Dominion KSX



Reading configuration.
Initializing hardware.
Initializing network communications.
Starting Dominion KSX.
Dominion KSX initialized successfully.

Press ENTER to login.
```

11. Congratulations! Dominion KSX is now ready for initial connection.

Proceed to the next section to initiate your first remote connection to Dominion KSX. After you have become familiar with the remote operation of Dominion KSX, consult **Chapter 4: Administrative Functions** to review the complete administrative functions provided by Dominion KSX.

Connect to Dominion KSX Remotely

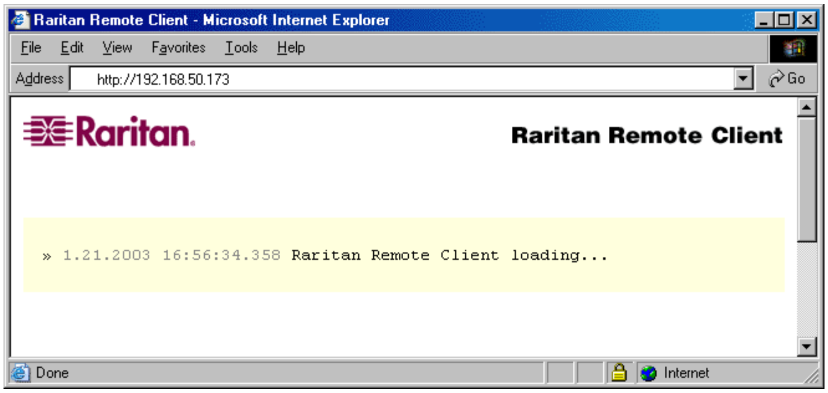
Having completed the physical installation of Dominion KSX, you are now ready to establish an initial network connection. Below are basic instructions for doing so. Please see **Chapter 3: Raritan Remote Client** for detailed instructions, being sure to review the "KVM Session Properties" and "Color Calibration" sections to optimize your Dominion KSX performance for Target KVM Servers.

Launch Raritan Remote Client (RRC)

1. Log into any Windows-based computer with network access to Dominion KSX.
2. If you are using Windows NT, 2000, XP, or 2003, ensure that you are not a "restricted" user.
3. Launch Microsoft Internet Explorer. Ensure that your Internet Explorer security settings allow the download and execution of ActiveX controls.

> ***Note:*** *The Windows default security setting, "Medium", will suffice.*

4. In the text field found on the Internet Explorer "Address" bar, type in the IP address you assigned to Dominion KSX in Step 6 of the previous section, "Initial Configuration." Press the <**Enter**> key to load and launch the web access client, called Raritan Remote Client.


Raritan Remote Client - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Go
Raritan
Raritan Remote Client
Done
Internet

http://192.168.50.173

» 1.21.2003 16:56:34.358 Raritan Remote Client loading...

5. After launching Raritan Remote Client, you will see a tree list on the left-hand side of the screen with a list of all automatically-detected Raritan devices found on your subnet. If you do not find your Dominion KSX unit listed there by name, create one manually by selecting **Connection → New Profile** on the menu bar. See **Chapter 3: Raritan Remote Client, *RRC Navigator*** and ***Creating New Profiles*** for more information.
6. Double-click on the entry corresponding to your Dominion KSX unit, found on the left-hand side of Raritan Remote Client.

Establish a Connection

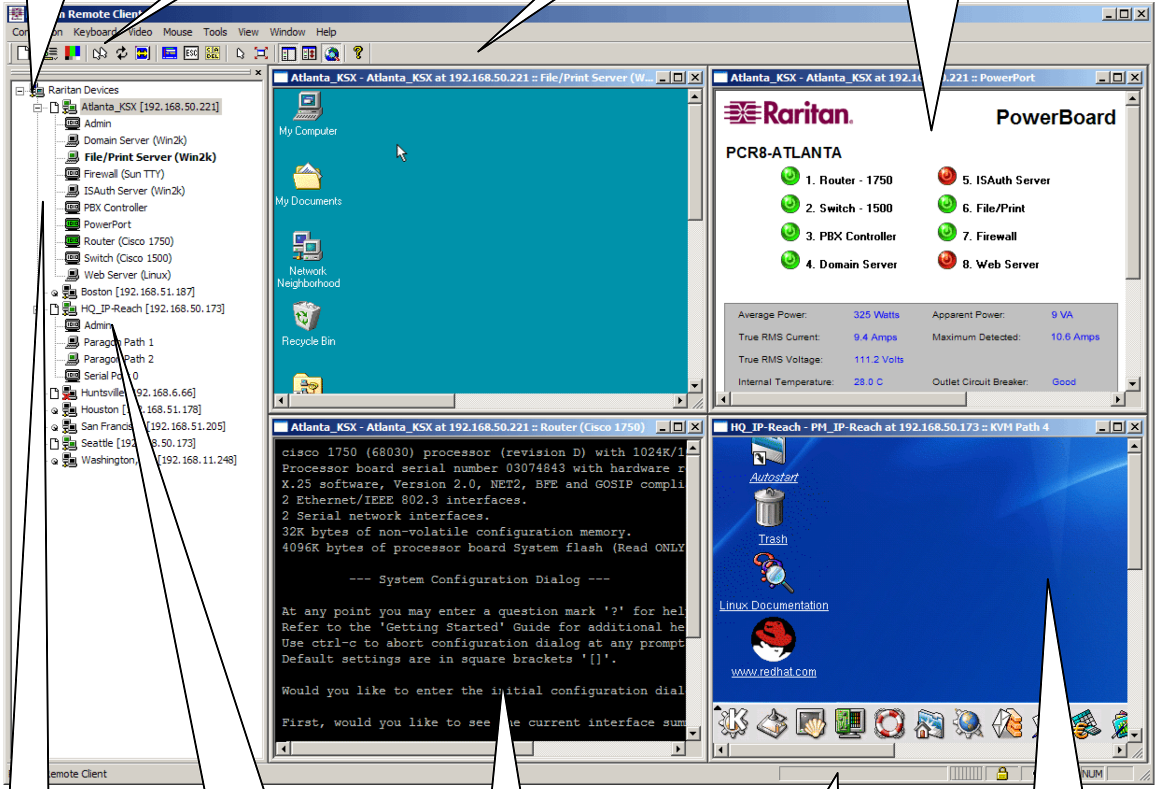
Immediately upon double-clicking on the entry corresponding to your Dominion KSX unit, found on the left-hand side of Raritan Remote Client (RRC), Dominion KSX will request your user credentials. (See your Dominion KSX User Manual for user account administration). Login with the default username and password ("admin"/"raritan"). You will immediately be connected to your Dominion KSX unit. Use the RRC Navigator, found on the left-hand side of the RRC window, to select and connect to a port.

The RRC Navigator displays any known Raritan networked appliances in a single view. Select **Connection → New Profile** to create new entries.

Click on "Synchronize Mouse" to converge the mouse pointers displayed in KVM windows.

The RRC Toolbar provides easy access to RRC's most frequently utilized features.

If a Raritan Remote Power Control Unit is attached to Dominion KSX, double-click on "PowerPort" in the RRC Navigator to invoke the graphical power control interface.



PCR8-ATLANTA

● 1. Router - 1750	● 5. ISAuth Server
● 2. Switch - 1500	● 6. File/Print
● 3. PBX Controller	● 7. Firewall
● 4. Domain Server	● 8. Web Server

Average Power:	325 Watts	Apparent Power:	9 VA
True RMS Current:	9.4 Amps	Maximum Detected:	10.6 Amps
True RMS Voltage:	111.2 Volts		
Internal Temperature:	28.0 C	Outlet Circuit Breaker:	Good

```
cisco 1750 (68030) processor (revision D) with 1024K/1
Processor board serial number 03074843 with hardware r
X.25 software, Version 2.0, NET2, BFE and GOSIP compli
2 Ethernet/IEEE 802.3 interfaces.
2 Serial network interfaces.
32K bytes of non-volatile configuration memory.
4096K bytes of processor board System flash (Read ONLY

         --- System Configuration Dialog ---

At any point you may enter a question mark '?' for hel
Refer to the 'Getting Started' Guide for additional he
Use ctrl-c to abort configuration dialog at any prompt
Default settings are in square brackets '[]'.

Would you like to enter the initial configuration dial

First, would you like to see he current interface sum
```

Double-click on any serial or KVM port to establish access to and control of the device attached.

RRC works with many different Raritan IP-based products, each of which may be configured remotely by double-clicking on the "Admin" port.

RRC provides VT100 console access to devices connected to the Serial Ports of Dominion KSX.

The RRC Status Bar provides real-time information on connection parameters.

When connected to a KVM console port, keystrokes and video signals are transmitted in real-time — exactly as if you were situated locally.

Chapter 3: Raritan Remote Client

Invoking Raritan Remote Client (RRC) via Web Browser

Dominion KSX features Web Browser access, providing a connection from any Windows-based Remote PC running Microsoft Internet Explorer 4.0+, Mozilla 1.1+, and Netscape 7+.

Security Settings

Accessing Dominion KSX via web browser requires your web browser to be configured to appropriate settings. Specifically, in the Internet Explorer security settings tab:

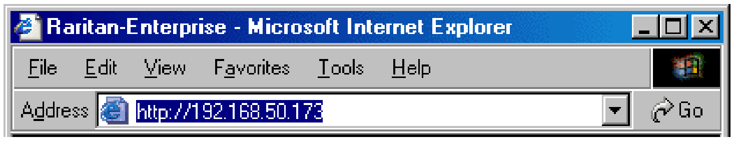
- “Download Signed ActiveX controls” should be set to either “Enable” or “Prompt”
- “Run ActiveX controls and plug-ins” should be set to either “Enable” or “Prompt”

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

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

Launching Raritan Remote Client

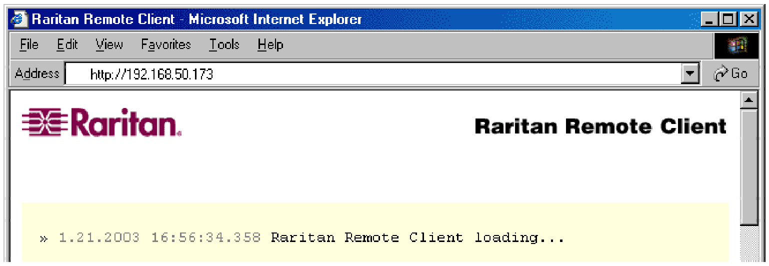
1. After checking to ensure that your browser security settings have been configured appropriately, type the IP address assigned to your Dominion KSX unit (see **Chapter 2: Installation, *Initial Configuration***) in the URL / Address text box of your web browser.


Raritan-Enterprise - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Go

http://192.168.50.173

Note: *Dominion KSX ships with the default IP address of 192.168.0.192*

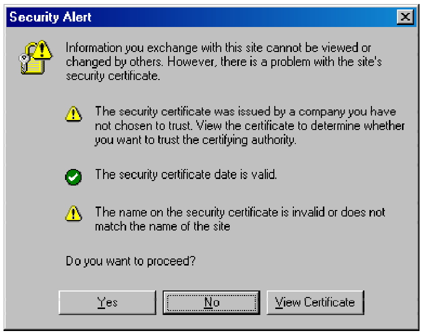
2. Dominion KSX will redirect you to an HTTPS (128-bit) secure web page for launching Raritan Remote Client.


Raritan Remote Client - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Go
Raritan
Raritan Remote Client

http://192.168.50.173

```
» 1.21.2003 16:56:34.358 Raritan Remote Client loading...
```

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



Security Alert

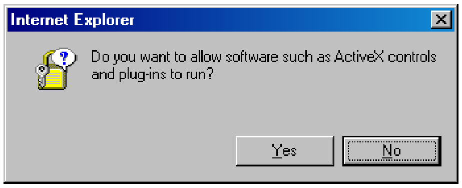
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

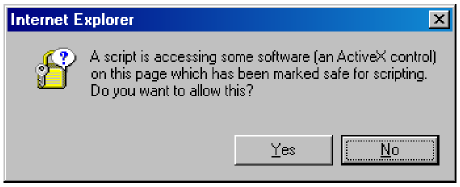
The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?



Internet Explorer

Do you want to allow software such as ActiveX controls and plug-ins to run?



Internet Explorer

A script is accessing some software (an ActiveX control) on this page which has been marked safe for scripting. Do you want to allow this?

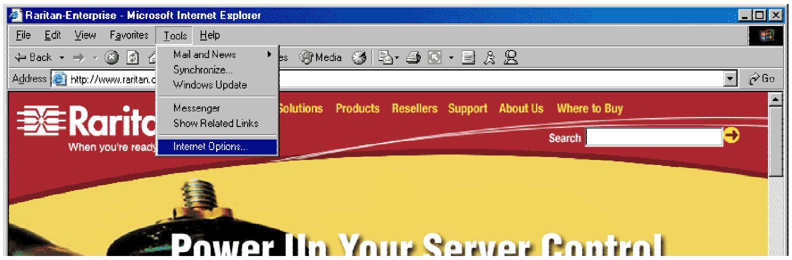
__Note__: Microsoft Windows 2000 and Microsoft Windows XP restrict certain types of users from downloading and running ActiveX controls and plug-ins, regardless of the settings in Internet Explorer and regardless of your approval of the above warnings. Please review the previous section, "Security Settings", and consult your Microsoft Windows documentation for more information.

Removing RRC From Browser Cache

If you ever wish to remove RRC from your browser cache, whether to perform an upgrade, to save disk space, or to remove evidence of RRC being executed on a PC, follow the standard procedure as proscribed by your web browser software.

Directions for Internet Explorer v6.0:

1. If you have used RRC recently, exit and restart Internet Explorer.
2. On the Internet Explorer menu bar, select **Tools → Internet Options**.



3. When the "Internet Options" dialog box appears, click on "Settings."
4. When the "Settings" dialog box appears, click on "View Objects."
5. Internet Explorer will display a list of cached program objects. Select any entries named "TeleControl Class", "Raritan Console", or "Power Board" and delete them.

Optional: Installing Raritan Remote Client Software

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

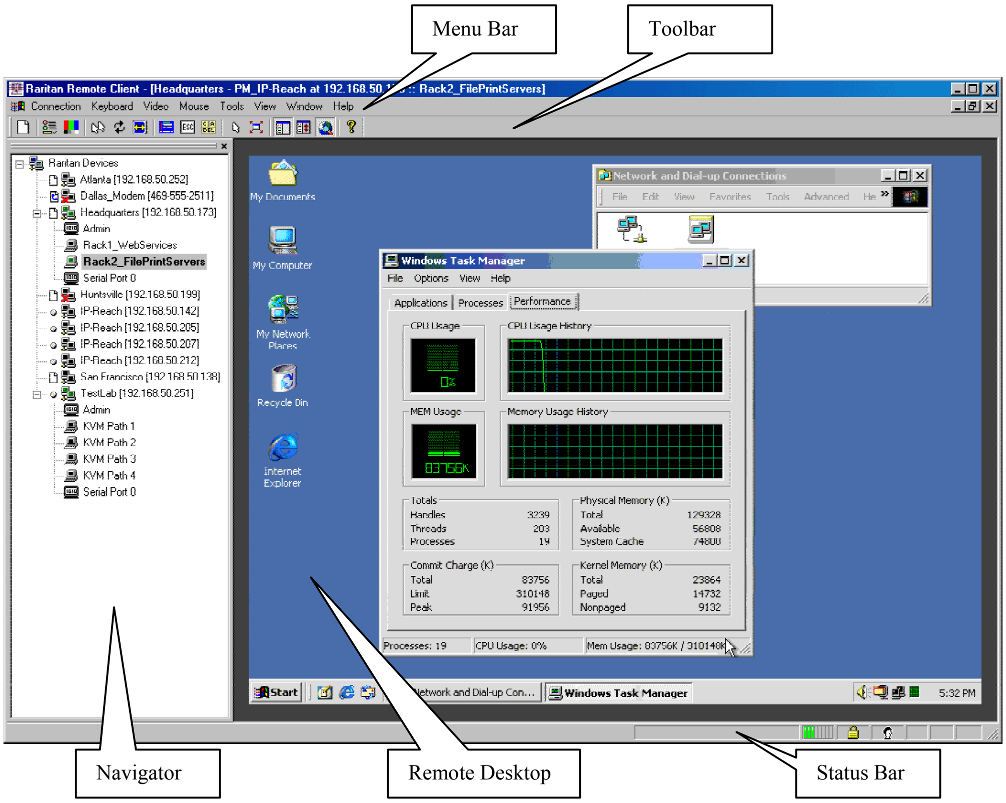
1. Insert the provided (RRC) CD-ROM into the CD-ROM drive of your PC. Make sure the RRC version indicated is v3.10 or greater.
2. The RRC setup program will run automatically. If it does not, right-click on your PC's CD-ROM drive in Windows Explorer and choose **Auto Play**.
3. Follow the on-screen instructions given by the InstallShield Wizard to complete TRC installation on your Remote PC. Under "Select Components," you must select either the US version for a US Remote PC keyboard, or the Japanese version for a Japanese Remote PC keyboard.

> ***Note:*** *The Japanese version of RRC enables a Japanese keyboard at the Remote PC and also requires a Japanese keyboard to be set at the Target Server. The interface information remains in English.*

4. Depending upon the configuration of your PC, the RRC installation program may also automatically install Direct X and Microsoft Foundation Class libraries if required. If this occurs, you will be directed to restart your PC upon completing installation.
5. A Raritan Remote Client icon will be added to your desktop. Click on this icon to launch Raritan Remote Client.

RRC Window Layout

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


Menu Bar
Toolbar
Raritan Remote Client - [Headquarters - PM_IP-Reach at 192.168.50.173 :: Rack2_FilePrintServers]
Connection Keyboard Video Mouse Tools View Window Help
Raritan Devices
Atlanta [192.168.50.252]
Dallas_Modem [469-555-2511]
Headquarters [192.168.50.173]
Admin
Rack1_WebServices
Rack2_FilePrintServers
Serial Port 0
Huntsville [192.168.50.199]
IP-Reach [192.168.50.142]
IP-Reach [192.168.50.205]
IP-Reach [192.168.50.207]
IP-Reach [192.168.50.212]
San Francisco [192.168.50.138]
TestLab [192.168.50.251]
Admin
KVM Path 1
KVM Path 2
KVM Path 3
KVM Path 4
Serial Port 0
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Network and Dial-up Connections
Windows Task Manager
Applications Processes Performance
CPU Usage
CPU Usage History
MEM Usage
Memory Usage History
Processes: 19 CPU Usage: 0% Mem Usage: 83756K / 310148K
Start
5:32 PM
Navigator
Remote Desktop
Status Bar

RRC Navigator

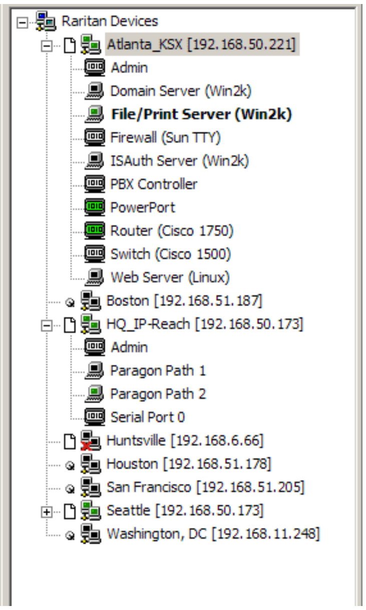
The RRC Navigator provides a single view to every known Raritan device, allowing convenient access to multiple Raritan networked appliances.

The RRC Navigator displays:

(a) All Raritan devices for which a *connection profile* exists, and

(b) All Raritan devices that are automatically identified on the network

> ***Note:*** *Automatic Raritan device identification utilizes the UDP protocol, and will typically identify all Raritan devices on your subnet. Network administrators rarely allow UDP to function outside of a subnet.*
>
> ***Note:*** *Automatic Raritan device identification will find only Raritan devices configured to use the default TCP Port (5000).*



- Raritan Devices
  - Atlanta_KSX [192.168.50.221]
    - Admin
    - Domain Server (Win2k)
    - **File/Print Server (Win2k)**
    - Firewall (Sun TTY)
    - ISAuth Server (Win2k)
    - PBX Controller
    - PowerPort
    - Router (Cisco 1750)
    - Switch (Cisco 1500)
    - Web Server (Linux)
  - Boston [192.168.51.187]
  - HQ_IP-Reach [192.168.50.173]
    - Admin
    - Paragon Path 1
    - Paragon Path 2
    - Serial Port 0
  - Huntsville [192.168.6.66]
  - Houston [192.168.51.178]
  - San Francisco [192.168.51.205]
  - Seattle [192.168.50.173]
  - Washington, DC [192.168.11.248]

Each device entry in the RRC Navigator provides two icons to communicate network status and connection profile information.

Left Icon (Connection Profile)

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

Right Icon (Network Status)

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

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

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

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

🖥	Remote KVM Port, connected (green)
🖥	Remote KVM Port, not yet connected
🖥	Remote Serial port, connected (green)
🖥	Remote Serial Port, not yet connected

Navigator Options

Certain RRC Navigator attributes may be customized to your preferences.

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

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

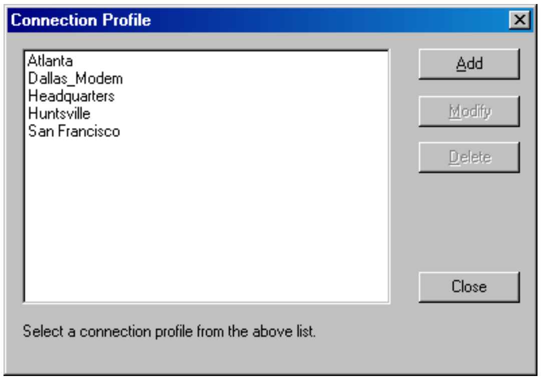
Creating New Profiles

Connection profiles store important information about your Raritan device such as IP Address, custom TCP ports, preferred compression settings, and custom security keys.

> ***Note:*** *If your Raritan device is configured to use a custom TCP port (see* ***Chapter 4: Administrative Functions,*** **Network Configuration***), or a group security key (see* ***Chapter 4: Administrative Functions,*** **Security Settings***), you must first create a connection profile in order to access the device.*

To Create a Connection Profile:

1. Select Connection → New Profile from the Menu Bar, or click on the leftmost icon in the Toolbar. The Connection Profile dialog box will appear, displaying all connection profiles which currently exist.



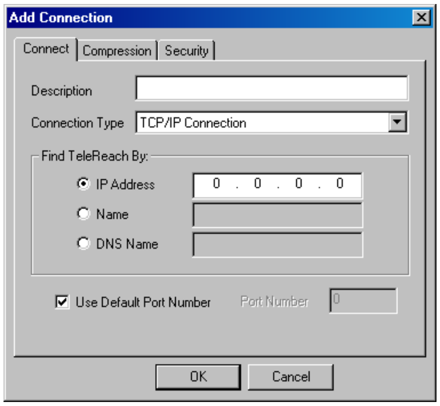
Connection Profile

Atlanta
Dallas_Modem
Headquarters
Huntsville
San Francisco

Select a connection profile from the above list.

2. Click on the [**Add**] button.
3. The Add Connection dialog appears, whose options are grouped into three tabs: **Connect**, **Compression**, and **Security.**

Connect Tab



Description

Connection Type: TCP/IP Connection

Find TeleReach By:

● IP Address 0 . 0 . 0 . 0

○ Name

○ DNS Name

☑ Use Default Port Number Port Number 0

- **Description**: Enter a text name to easily identify the Raritan device that you are configuring, such as "Atlanta_Datacenter."
- **Connection Type**: Select **TCP/IP Connection** for a LAN/WAN connection; select **Dial-Up Connection** for a direct analog modem connection to the Raritan device.

For a TCP/IP Connection, select the manner by which RRC should locate your Raritan device:

- **IP Address**: The IP address assigned to your Raritan device (see **Chapter 4: Administrative Functions, *Network Configuration***).
- **Name**: The name assigned to your Raritan device during initial setup (see **Chapter 4: Administrative Functions, *Network Configuration***).

> ***Note:*** *If dynamic DHCP addressing is used for Dominion KSX, then* ***Find Dominion KSX by Name*** *should be used.*
>
> ***Note:*** *The factory default unit name for each Dominion KSX produced is <Dominion KSX>. To change the default name on a Dominion KSX unit and institute a unique name, see* ***Chapter 4.***

- **DNS Name**: If you have configured your DNS server to resolve a DNS name to the IP address that you have assigned to your Raritan device, you may use this DNS name to access your Raritan device.

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

- **Phone Number**: Be sure to include any additional codes that RRC should dial to establish a connection, such as country codes, area codes, outside line access codes, etc.
- **Modem**: Select the modem, as configured in Windows, that RRC should use to dial and connect to your Raritan device.

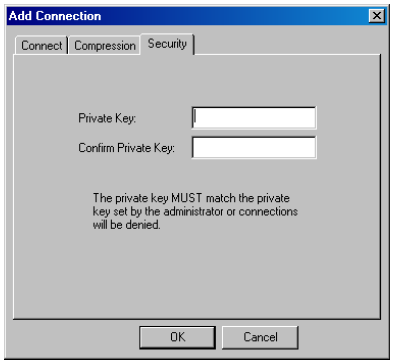
Select a TCP Port to use:

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

Compression Tab

Settings in the Compression Tab are adjustable via the RRC client, and therefore are not necessary for pre-configuration in the Connection Profile. Should you wish to pre-configure these settings, however, refer to the section in this chapter labeled "**Remote Desktop: KVM Console Control**, **Connection and Video Properties**."

Security Tab



The private key MUST match the private key set by the administrator or connections will be denied.

If you have configured your Dominion KSX unit to use a private group key, you must enter it here in order to be authorized to initiate a connection with that Dominion KSX unit. Click on the [**OK**] button when you have completed the fields.

When you have completed the Connect and Security screens, click on the [**OK**] button to finish creating the connection.

Establishing a New Connection

To connect to a Raritan networked device, simply double-click on its entry in the RRC Navigator. You will be asked to authenticate to the device.

> ***Note:*** *The default Dominion KSX login user name is <admin>, with the password <raritan>. This user has administrative privileges. Passwords are case sensitive and must be entered in the exact case combination in which they were created.*
> *The default password <raritan> must be entered entirely in lowercase letters.*
> *To ensure security, change the default username password as soon as possible.*

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

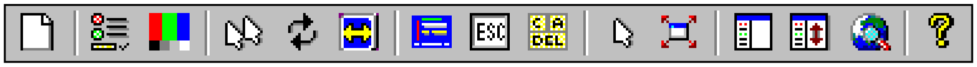
If you are having problems connecting to a Raritan device, be sure to check the following:

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

Closing a Remote Connection

When you would like to terminate your connection to a Dominion KSX unit, simply right-click on the device entry in the RRC Navigator, and select **Disconnect**.

RRC Toolbar and Shortcuts



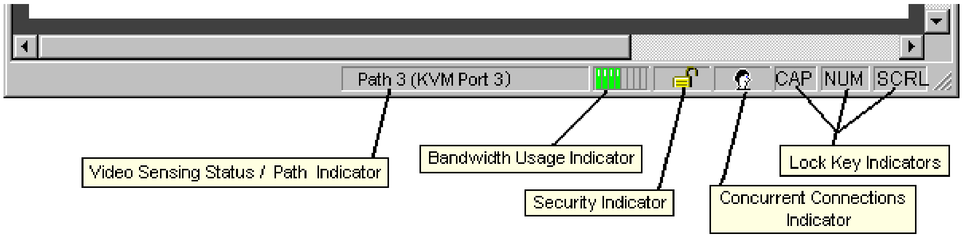
Raritan Remote Client Toolbar

The RRC Toolbar provides convenient, one-click access to the most commonly used features and parameters of Raritan Remote Client:

BUTTON	BUTTON NAME	HOTKEY	FUNCTION
🗋	New Profile	<Ctrl+Alt+C>	Creates a new Navigator entry for a Raritan device; same results as selecting **Connection → New Profile** in the menu bar.
☰	Connection Properties	<Ctrl+Alt+P>	Opens Modify Connection Properties dialog box to manually adjust bandwidth-correlated options (Connection Speed, Color Depth, etc.).
🟥🟩🟦	Video Settings	N/A	Opens the Video Settings dialog box to manually adjust video conversion parameters.
⇆	Synchronize Mouse	<Ctrl+Alt+S>	In dual-mouse mode, forces realignment of Target Server mouse pointer with Raritan Remote Client mouse pointer.
⟳	Refresh Screen	<Ctrl+Alt+R>	Forces refresh of video screen.
⟷	Auto-sense Video Settings	<Ctrl+Alt+A>	Forces refresh of video settings (resolution, refresh rate).
☰	Enter On-Screen Menu	N/A	Not applicable for Dominion KSX. Used by RRC with other Raritan products.
ESC	Exit On-Screen Menu	ESC	Not applicable for Dominion KSX. Used by RRC with other Raritan products.
C A DEL	Send Ctrl+Alt+Del	<Ctrl+Alt+D>	Not applicable for Dominion KSX. Used by RRC with other Raritan products.
⇖	Single Cursor Mode	<Ctrl+Alt+X>	Enters Single Cursor Mode, in which the local PC's mouse pointer no longer appears on-screen. Press <Ctrl+Alt+X> to exit this mode.
⛶	Full Screen Mode	<Ctrl+Alt+F>	Maximizes the screen real estate to view the Target Server desktop.
◧	Show / Hide Navigator	N/A	Toggles whether or not the RRC Navigator is displayed.
↕	Refresh Navigator	N/A	Forces a refresh of the data displayed by the RRC Navigator.
🌐	Show / Hide "Browsed" Devices	N/A	Toggles whether or not the RRC Navigator displays Raritan Devices automatically identified on the network (that do not have pre-configured profiles associated with them).
?	About	N/A	Displays version information about Raritan Remote Client.

RRC Status Bar

The **Status Bar** at the bottom of the Raritan Remote Client window conveys information about the status of your remote connection session to Dominion KSX.


Path 3 (KVM Port 3)
CAP
NUM
SCRL
Video Sensing Status / Path Indicator
Bandwidth Usage Indicator
Security Indicator
Concurrent Connections Indicator
Lock Key Indicators

Video Sensing Status / Path Indicator

Indicates the occurrence of video sensing, during connections to Target KVM Server ports.

Bandwidth Usage Indicator

Indicates how much of your total available bandwidth is currently being used. The **Connection Speed** setting, found under the Compression tab of the Connection Properties screen, determines total available bandwidth.

Security Indicator

Indicates whether the current remote connection is protected by encryption. Encryption requirements are set during Dominion KSX configuration (see **Chapter 4**). When a Dominion KSX device is configured for **No encryption** or **SSL Authentication, NO data encryption**, the Security Indicator is represented on the Status Bar as an open lock. When **SSL authentication, data encryption** or **SSL authentication, SSL encryption** is selected, the Security Indicator is represented on the Status Bar as a closed lock.

Concurrent Connections Indicator

Indicates if multiple remote users are currently connected to the same Dominion KSX path, showing one icon for a single connected user, and two icons if two or more users are connected.

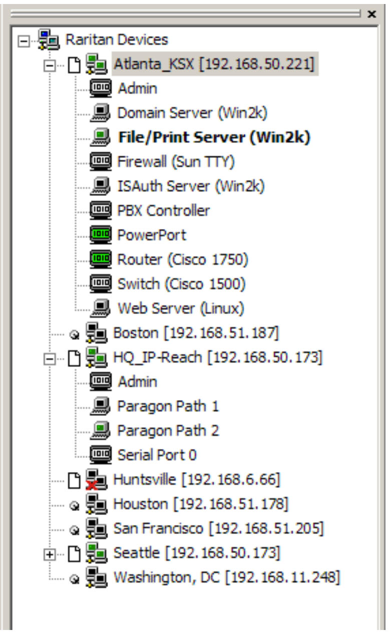
Concurrent connection ability can be set globally under **PC Share Mode** on the Security Configuration screen (see **Chapter 4**), or set per individual user in the **Concurrent Access Mode** setting on the User Account Settings screen (see **Chapter 4**).

Lock Key Indicators

Indicates the status of the current Target KVM Server, with respect to the activation of the Caps-Lock, Num-Lock, and Scroll-Lock keys. If these keys are enabled on the Target Server being viewed, this affirmative status will be reflected on the Status Bar as indicated.

Remote Desktop: KVM Console Control

After using the RRC Navigator to establish a connection with a Dominion KSX unit (see the previous section: **Establishing a Connection**), the Navigator entry corresponding to the Dominion KSX unit will expand to show all ports on the Dominion KSX enabled for remote access.



Remote KVM ports are designated with the following icon:

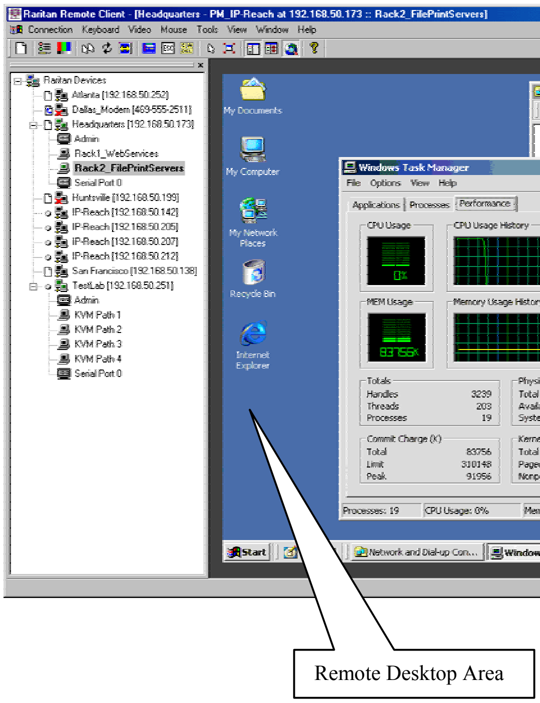
To establish a remote KVM console connection, simply double-click on the KVM port that you would like to control.

Upon connection, Dominion KSX displays the real-time video output by the Target KVM Server that is connected to your Dominion KSX KVM port. This video is compressed and encrypted according to the configuration settings specified by the administrator (see **Chapter 4**).

Once connected to a Target KVM server, you obtain complete, low-level control of the KVM console as if you were physically located next to the server.

To switch to a different KVM port, simply double-click on the corresponding entry in the RRC Navigator.

When your mouse pointer lies within the Remote Desktop area of RRC, mouse movements and clicks are directly transmitted to the Target KVM server connected.


Raritan Remote Client - [Headquarters - PM_IP-Reach at 192.168.50.173 :: Rack2_FilePrintServers]
Connection Keyboard Video Mouse Tools View Window Help
Raritan Devices
Atlanta [192.168.50.252]
Dallas_Modem [469-555-2511]
Headquarters [192.168.50.173]
Admin
Rack1_WebServices
Rack2_FilePrintServers
Serial Port 0
Huntsville [192.168.50.199]
IP-Reach [192.168.50.142]
IP-Reach [192.168.50.205]
IP-Reach [192.168.50.207]
IP-Reach [192.168.50.212]
San Francisco [192.168.50.138]
TestLab [192.168.50.251]
Admin
KVM Path 1
KVM Path 2
KVM Path 3
KVM Path 4
Serial Port 0
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Network and Dial-up Connections
Windows Task Manager
File Options View Help
Applications Processes Performance
CPU Usage
CPU Usage History
MEM Usage
Memory Usage History
Start
Network and Dial-up Con...
Windows Task Manager
5:32 PM
Remote Desktop Area

Single Mouse Mode / Dual Mouse Mode

When remotely viewing a Target KVM Server that uses a pointing device, by default you will see two mouse pointers within the Remote Desktop area of the Raritan Remote Client window. The Raritan Remote Client mouse pointer, generated by the operating system on which RRC is running, slightly leads the Target KVM Server's mouse pointer during movement, a necessary result of digital delay.

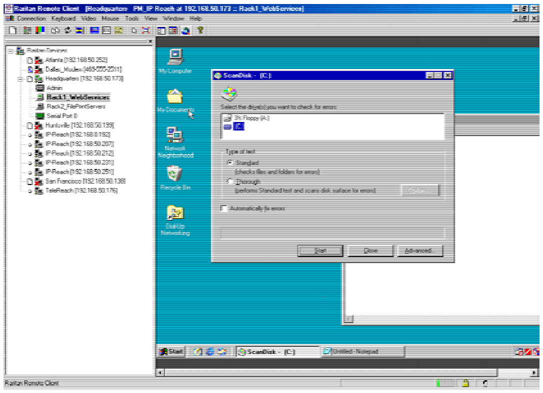
On fast LAN connections, however, some users prefer to disable the Raritan Remote Client mouse pointer, opting to view only the Target KVM Server's mouse pointer during operation. To toggle between these two modes, use the <**Ctrl+Alt+X**> hotkey, or press the **Single Mouse Pointer** mode icon in the RRC Toolbar.

*__Note:__ For better alignment between the two mouse pointers in dual-mouse mode, click on the [**Synchronize Mouse**] button on the RRC Toolbar, or simultaneously press the keys <**Ctrl+Alt+S**>. This will force a realignment of the two mouse pointers. If you have carefully followed the "Configuring Target KVM Servers" directions found in Chapter 2, and the mouse pointers still remain out of sync, click on the [**Auto-Sense Video**] button on the RRC Toolbar.*

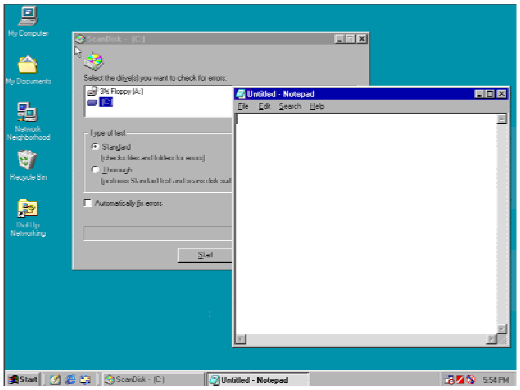
Full Screen Mode

Raritan Remote Client's full screen mode maximizes the screen real estate available to RRC for displaying the remote desktop by removing window borders, toolbars, status bars, and the RRC Navigator.

This option is particularly useful for viewing a Target KVM Server whose video resolution is equal to or greater than the video resolution setting of the PC on which RRC is running, for example, viewing a 1028x768 server on a 1028x768 PC.


Raritan Remote Client [Headquarters: PM_IP Reach at 192.168.50.173 :: Rack1_WebServices]
Connection Keyboard Video Mouse Tools View Window Help
Raritan Devices
Atlanta [192.168.50.252]
Dallas_Modem [469-555-2511]
Headquarters [192.168.50.173]
Admin
Rack1_WebServices
Rack2_FilePrintServers
Serial Port 8
Huntsville [192.168.50.139]
IP-Reach [192.168.0.152]
IP-Reach [192.168.50.207]
IP-Reach [192.168.50.212]
IP-Reach [192.168.50.231]
IP-Reach [192.168.50.251]
San Francisco [192.168.50.138]
TeleReach [192.168.50.176]
My Computer
My Documents
Network Neighborhood
Recycle Bin
Dial-Up Networking
ScanDisk - (C:)
Select the drive(s) you want to check for errors:
3½ Floppy (A:)
(C:)
Type of test
Standard
(checks files and folders for errors)
Thorough
(performs Standard test and scans disk surface for errors)
Options...
Automatically fix errors
Start
Close
Advanced...
Start
ScanDisk - (C:)
Untitled - Notepad
Raritan Remote Client

Standard View



Full Screen Mode View

To toggle full screen mode, click on the full screen mode icon in the RRC Toolbar (or press the hotkey combination Ctrl+Alt+F). To exit full screen mode, press the hotkey combination Ctrl+Alt+F.

Keyboard Macros

RRC allows users to create custom keyboard macros in order to send given key sequences to the Target KVM Server connected to Dominion KSX. This feature allows customers to send keystrokes to remote servers that may be otherwise unintentionally interpreted by the computer on which RRC is running.

Dominion KSX's Keyboard Macro feature can be used to ensure that keystroke combinations intended for the Target Server are sent to, and interpreted only by, the Target Server.

Ctrl+Alt+Delete Macro

Due to its frequent use, a Ctrl+Alt+Delete macro has been pre-programmed into Raritan Remote Client, and is useful in illustrating the power of keyboard macros.

C A DEL	Send Ctrl+Alt+Del	<Ctrl+Alt+D>	Sends a Ctrl+Alt+Delete macro to the Target Server.

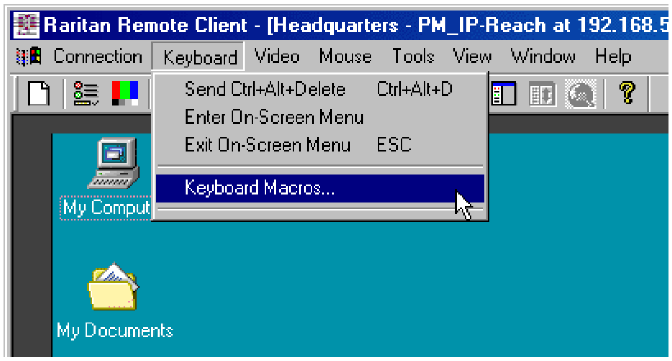
Clicking on the Ctrl+Alt+Delete icon in the RRC Toolbar sends this key sequence to the server or KVM switch to which you are currently connected. In contrast, if you were to physically press the Ctrl+Alt+Delete keys while using RRC, the command would first be intercepted by your own PC due to the structure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

Building a Keyboard Macro

To illustrate the creation of a keyboard macro, the following directions detail the steps necessary to create a keyboard macro for the Windows command, "Minimize All Windows / Show Desktop".

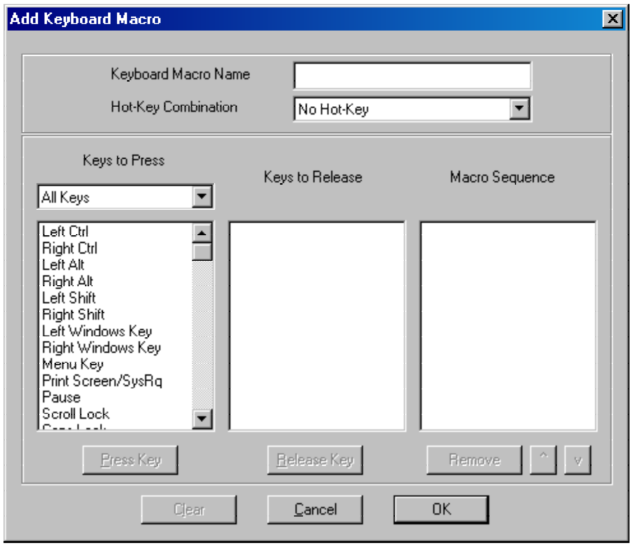
Example: In Windows, pressing the <**Windows+D**> key combination minimizes all program windows. However, when connected to a target server with RRC, a keyboard macro is the only means to accomplish this task on the target server – because, again, pressing the key combination <**Windows+D**> would result in your own client PC intercepting the command and performing it – instead of sending the command to the target server as intended.

1. On the RRC Menu Bar, select **Keyboard → Keyboard Macros**.



2. When the Keyboard Macros dialog box opens, click on the [**Add**] button.

3. The Add Keyboard Macro dialog box opens.



Hot-Key Combination: No Hot-Key

4. Build the Keyboard Macro by editing all the fields in the Add Keyboard Macro window, in the order described below. Click on the [**OK**] button when finished.

   a) Enter a name into the Keyboard Macro Name field, which will appear on the RRC Menu Bar, after successful creation of the keyboard macro. For our example, "Minimize All Windows".

   b) **Optional**: Designate a keystroke combination in the Hot-Key Combination field, which allows easy macro execution from your keyboard when RRC is running. For our example "Minimize All Windows," we selected <Ctrl+Alt+1>.

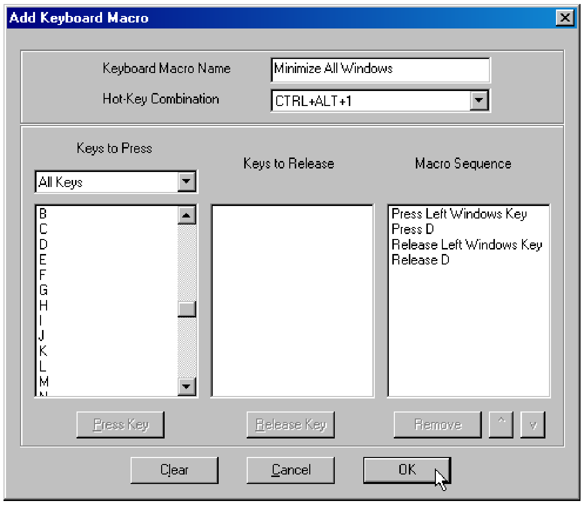
   c) In the **Keys to Press** selection box, select each key for which you would like to emulate key presses – in the order by which they are to be pressed – clicking on the [**Press Key**] button after each selection. As each key is selected, it will appear in the **Keys to Release** selection box in the middle of the dialog box.

   d) In our "Minimize All Windows" example, we require the transmission of two keys: the <**Windows**> key and the letter <**D**> key.

   e) In the **Keys to Release** selection box, select each key for which you would like to emulate key releases – in the order by which they are to be released – clicking on the [**Release Key**] button after each selection.

   f) In our "Minimize All Windows" example, we require both keys pressed to also be released.

   g) Review the **Macro Sequence** text box, whose contents are automatically generated, to ensure that the contents accurately reflect the exact key sequence you desire. Use the [**Remove**] and the arrow buttons to adjust the contents and order of your macro if necessary.

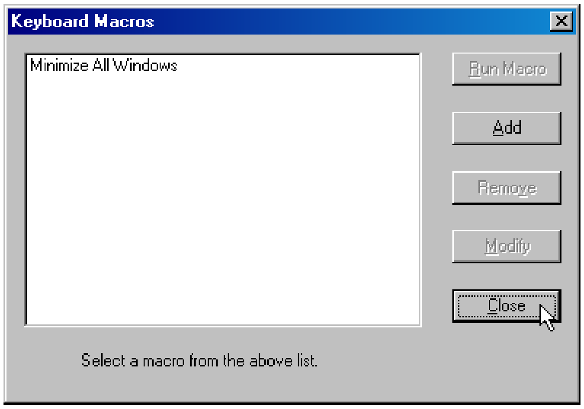


Keyboard Macro Name: Minimize All Windows

Hot-Key Combination: CTRL+ALT+1

Macro Sequence:
Press Left Windows Key
Press D
Release Left Windows Key
Release D

5. After clicking the [**OK**] button, the Keyboard Macros dialog box will appear, listing your new keyboard macro.



Minimize All Windows

Select a macro from the above list.

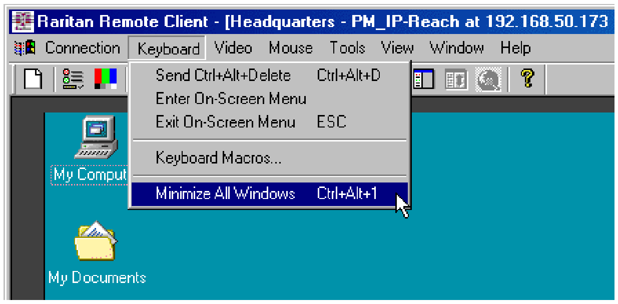
6. Click on the [**Close**] button to complete the keyboard macro editing procedure.

Running a Keyboard Macro

Once a macro is created, it can be run via the RRC Menu Bar or with the hotkey combination if one had been designated during the macro creation.

Menu Bar Activation

After a macro has been created, it appears in the Keyboard menu on the RRC Menu Bar. You can simply click on the entry to execute your new keyboard macro.


Raritan Remote Client - [Headquarters - PM_IP-Reach at 192.168.50.173
Connection
Keyboard
Video
Mouse
Tools
View
Window
Help
Send Ctrl+Alt+Delete Ctrl+Alt+D
Enter On-Screen Menu
Exit On-Screen Menu ESC
Keyboard Macros...
Minimize All Windows Ctrl+Alt+1
My Comput
My Documents

Hot-Key Activation

Alternatively, once a macro has been created, it can be executed while using RRC by pressing the hotkey you (optionally) assigned to the macro. In the "Minimize All Windows" example described above, a user can press the keys <**Ctrl+Alt+1**> simultaneously while using RRC to send the <**Windows+D**> key combination to the target server.

Connection and Video Properties

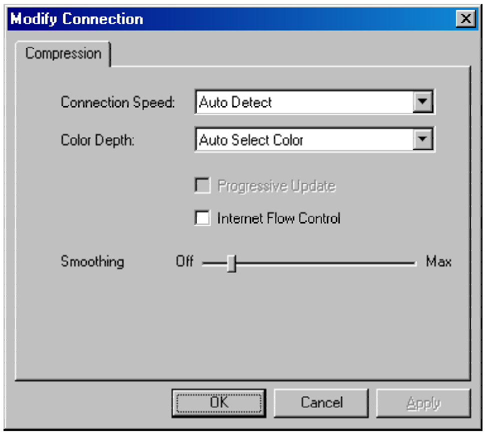
Dominion KSX's dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. Unlike competitive solutions, Dominion KSX optimizes its KVM output for not only LAN utilization, but also via the WAN and dial-up. By dynamically adjusting color depth and limiting video output, Dominion KSX offers the optimal balance between video quality and system responsiveness in any bandwidth constraint.

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

Connection Properties

	Connection Properties	<Ctrl+Alt+P>	Opens Modify Connection Properties dialog box to manually adjust bandwidth-correlated options (Connection Speed, Color Depth, etc.).

To access the Connection Properties dialog box, either select **Connection → Connection Properties** from the RRC Menu Bar, or click on the [**Connection Properties**] button in the RRC Toolbar.



Connection Speed: Auto Detect

Color Depth: Auto Select Color

□ Progressive Update

□ Internet Flow Control

Smoothing Off Max

Connection Speed

The Connection Speed selection box allows users to manually constrain Dominion KSX from using more than a designated amount of network bandwidth. While Dominion KSX normally detects available bandwidth automatically , users can use the Connection Speed setting to manually inform Dominion KSX of a bandwidth constraint – whereby Dominion KSX adapts its behavior and simply refrains from even attempting to consume more than the available bandwidth.

Color Depth

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

Instead, Dominion KSX can dynamically adapt the color depth transmitted to remote users, in order to maximize usability in all bandwidth constraints.

- **Progressive Update** option**:** The extremely innovative Dominion KSX feature of Progressive Update can enormously increase usability in constrained bandwidth environments. When Progressive Update is enabled, Dominion KSX first sends an image of the remote desktop at lower color depths, and then provides higher color depth images as bandwidth allows.

  This option is very similar in philosophy as the common World Wide Web notion of "interlaced GIF" files.

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

Internet Flow Control

Many public WAN links are by their very nature unpredictable. Packets sent over the public Internet do not necessarily arrive at their destination in the order they were sent. When using Dominion KSX over an unpredictable public WAN (particularly in international scenarios), the Internet Flow Control toggle ensures that packets transmitted by Dominion KSX are received and reconstructed by RRC in the correct order.

Smoothing

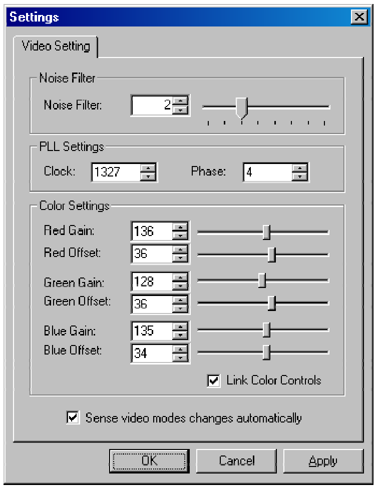
The video smoothing level instructs Dominion KSX to what degree color gradation shifts are relevant for transmission. Video pixels that stray from the majority color are assigned approximated color values to reduce bandwidth used and video noise transmitted. Overly high smoothing levels can result in color inaccuracies; whereas lower smoothing levels require greater bandwidth and processing power.

Video Settings

🟥🟩🟦	Video Settings	N/A	Opens the Video Settings dialog box to manually adjust video conversion parameters.

To access the Video Settings dialog box, either select **Video → Video Settings** from the RRC Menu Bar, or click on the [**Connection Properties**] button in the RRC Toolbar.

Most of the settings in this dialog box can be refreshed by performing Color Calibration, as described in the next section, or by manually forcing Dominion KSX to auto-detect the video settings (on the RRC Menu Bar, select **Video → Auto-sense Video Settings**). However, it is useful for power users to understand the meanings and ramifications of each setting.



Noise Filter

Noise Filter: 2

PLL Settings

Clock: 1327

Phase: 4

Color Settings

Red Gain: 136

Red Offset: 36

Green Gain: 128

Green Offset: 36

Blue Gain: 135

Blue Offset: 34

☑ Link Color Controls

☑ Sense video modes changes automatically

Noise Filter

The video output of graphics cards are transmitted in analog form, and are susceptible to electrical and interference noise. Dominion KSX's advanced circuitry can filter out these small, false, and unintended signal variations, thereby optimizing picture quality and bandwidth consumed.

Higher: Noise Filter settings instruct Dominion KSX to transmit a variant pixel of video only if a large color variation exists in comparison to its neighbors. However, setting the threshold too high can result in the unintentional filtering of desired screen changes.

Lower: Noise Filter settings instruct Dominion KSX to transmit most pixel changes. Setting this threshold too low results in higher bandwidth utilization.

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

Analog-to-Digital Settings

The following parameters are best left to Dominion KSX to automatically detect (on the RRC Menu Bar, select **Video > Auto-sense Video Settings**), but a brief description of each is included here.

- **PLL Settings**: If the video image looks extremely blurry or unfocused, the PLL Settings for clock and phase can be adjusted until a better image appears on the active Target Server.
  - **Clock:** Horizontal sync divider to produce pixel clock. Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended.
  - **Phase:** Phase values range from 0 to 31 and will wrap around. Stop at the phase value that results in the best video image for the active Target Server.
- **Color Settings:** Gain control can be thought of as contrast adjustment. Offset control can be thought of as brightness adjustment.
  - **Red Gain:** Controls the amplification of the red signal.
  - **Red Offset:** Controls the bias of the red signal.
  - **Green Gain:** Controls the amplification of the green signal.
  - **Green Offset:** Controls the bias of the green signal.
  - **Blue Gain:** Controls the amplification of the blue signal.
  - **Blue Offset:** Controls the bias of the blue signal.
  - **Link Color Controls:** Makes all the gain slide adjusters move in unison when any one color's gain slide is moved and all the offset slide adjusters move in unison when any one color's offset slide is moved.
- **Sense video mode changes automatically:** Determines whether Dominion KSX will automatically update the video image being sent RRC each time it detects a change in video resolution or refresh rates at the Target Server.

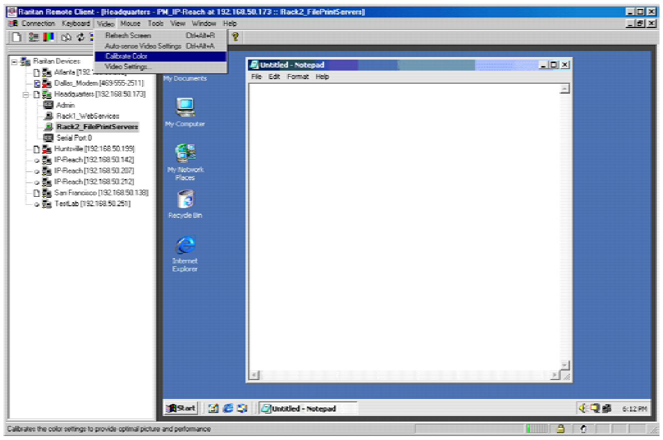
Color Calibration

Automatic Color Calibration adjusts the color settings on Dominion KSX to reduce excess color noise and data during digitization of video images. This data streamlining will increase the operational performance of Dominion KSX, particular color accuracy.

A very simple procedure to execute, Color Calibration should be performed if the color levels (hue, brightness, saturation) of transmitted video images do not seem accurate. Because Dominion KSX color settings remain static and do not change when switching from one Target KVM Server to another, performing this Color Calibration routine once on a single representational Target KVM Server will benefit all connected Target KVM Servers.

To Perform Color Calibration:

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. One simple way to accomplish this is to open the Notepad application and maximize its window size.


Raritan Remote Client - [Headquarters - PM_IP-Reach at 192.168.50.173 :: Rack2_FilePrintServers]
Connection
Keyboard
Video
Mouse
Tools
View
Window
Help
Refresh Screen Ctrl+Alt+R
Auto-sense Video Settings Ctrl+Alt+A
Calibrate Color
Video Settings...
Raritan Devices
Atlanta [192
Dallas_Modem [469-555-2511]
Headquarters [192.168.50.173]
Admin
Rack1_WebServices
Rack2_FilePrintServers
Serial Port 0
Huntsville [192.168.50.199]
IP-Reach [192.168.50.142]
IP-Reach [192.168.50.207]
IP-Reach [192.168.50.212]
San Francisco [192.168.50.138]
TestLab [192.168.50.251]
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Untitled - Notepad
File
Edit
Format
Help
Start
Untitled - Notepad
6:12 PM

Calibrates the color settings to provide optimal picture and performance

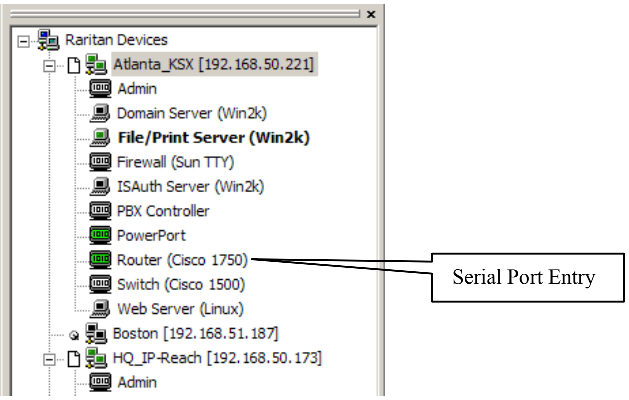
3. On the RRC Menu Bar, select **Video → Calibrate Color** to perform the color calibration.

Remote Desktop: Serial Control

In addition to remote KVM console access, Dominion KSX also offers users the convenience of accessing your remote serial devices with the same solution. Any serial console supporting VT100 emulation may be connected to the serial ports found on Dominion KSX, and accessed using the Raritan Remote Client.

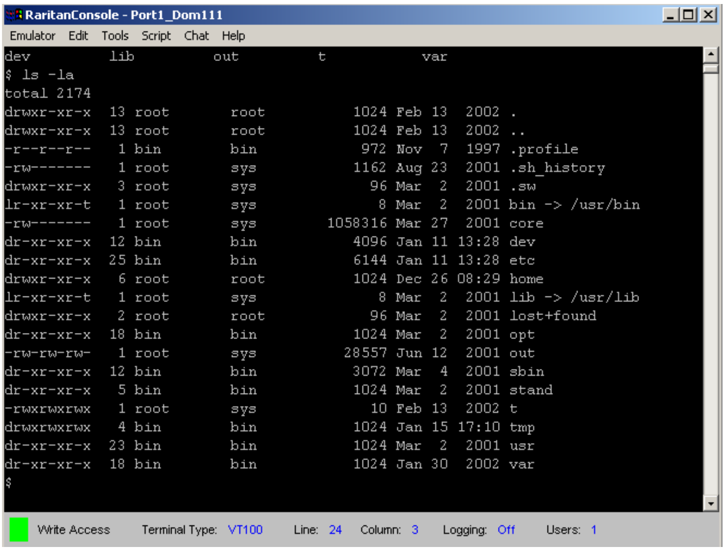
Remote Connection

To open a remote connection to a serial device connected to your Dominion KSX, double-click on the corresponding Navigator entry as displayed by RRC:



Remote Serial Ports are designated with the following icon:

A terminal window displaying the console output of the serial device connected to Dominion KSX will appear, and the icon found next to the serial port entry on the RRC Navigator will turn green.



```
dev          lib          out          t            var
$ ls -la
total 2174
drwxr-xr-x  13 root       root          1024 Feb 13  2002 .
drwxr-xr-x  13 root       root          1024 Feb 13  2002 ..
-r--r--r--   1 bin        bin            972 Nov  7  1997 .profile
-rw-------   1 root       sys           1162 Aug 23  2001 .sh_history
drwxr-xr-x   3 root       sys             96 Mar  2  2001 .sw
lr-xr-xr-t   1 root       sys              8 Mar  2  2001 bin -> /usr/bin
-rw-------   1 root       sys        1058316 Mar 27  2001 core
dr-xr-xr-x  12 bin        bin           4096 Jan 11 13:28 dev
dr-xr-xr-x  25 bin        bin           6144 Jan 11 13:28 etc
drwxr-xr-x   6 root       root          1024 Dec 26 08:29 home
lr-xr-xr-t   1 root       sys              8 Mar  2  2001 lib -> /usr/lib
drwxr-xr-x   2 root       root            96 Mar  2  2001 lost+found
dr-xr-xr-x  18 bin        bin           1024 Mar  2  2001 opt
-rw-rw-rw-   1 root       sys          28557 Jun 12  2001 out
dr-xr-xr-x  12 bin        bin           3072 Mar  4  2001 sbin
dr-xr-xr-x   5 bin        bin           1024 Mar  2  2001 stand
-rwxrwxrwx   1 root       sys             10 Feb 13  2002 t
drwxrwxrwx   4 bin        bin           1024 Jan 15 17:10 tmp
dr-xr-xr-x  23 bin        bin           1024 Mar  2  2001 usr
dr-xr-xr-x  18 bin        bin           1024 Jan 30  2002 var
$
```

🟩 Write Access   Terminal Type: VT100   Line: 24   Column: 3   Logging: Off   Users: 1

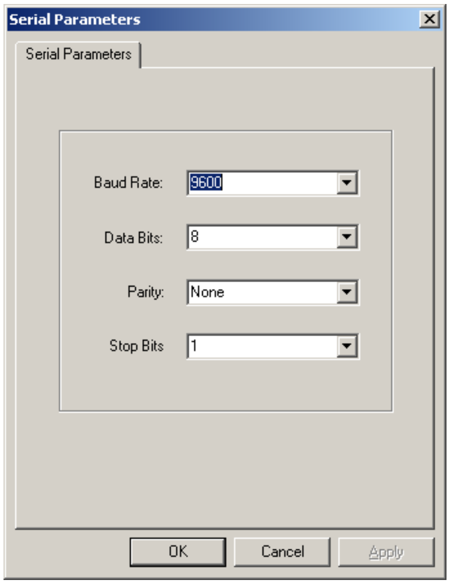
Note: *Dominion KSX Serial Console access supports only VT100 terminal emulation; be sure your serial device is appropriately configured before connecting to Dominion KSX.*

Note: *If using Windows XP, Service Pack 1, the serial console will not appear if you have two conflicting Java virtual machines installed on your system (i.e., one from Sun Microsystems, and on from Microsoft).*

Upon connecting remotely to the selected serial console port, your keystrokes will be transmitted directly to that serial console port.

Changing Serial Settings

You may change the serial terminal settings such as baud rate, parity, and stop bits used by Dominion KSX to communicate with your serial device, by right-clicking on the serial port entry in the RRC Navigator, and selecting **Serial Parameters** in the menu. Click on the [**OK**] button when finished.



Baud Rate: 9600
Data Bits: 8
Parity: None
Stop Bits 1

Viewing Serial Console History

The History feature allows you to view the recent history of your console sessions by displaying the console messages to and from the target device. This function displays up to 999 lines of recent console message history. This information can be useful during debugging, troubleshooting, or administering a target device.

Note*: History data is displayed only to the user who requested the history.*

To View Session History:

1. In the top menu bar of Raritan Remote Console, click on **Serial**.
2. Select *History* from the drop-down menu.

Serial Console Logging

Raw console data from the target device can be logged to a file in your computer.

Start Logging

1. In the top menu bar of Raritan Remote Console, click on **Serial**.
2. Select *Start Logging* from the drop-down menu.
3. Choose an existing file or provide a new file name in the File Dialog box. When an existing file is selected for logging, data gets appended to the contents. Providing a new file name creates a brand new file. Click on the [**OK**] button after you have selected or created a file.

Stop Logging

1. In the top menu bar of Raritan Remote Console, click on **Serial**.
2. Select *Stop Logging* from the drop-down menu.

Cutting and Pasting Serial Data

Use the Copy, Paste, and Select All Text commands to relocate and / or re-use important text.

To Copy and Paste All Text:

1. In the top menu bar of Raritan Remote Console, click on **Serial**.
2. Choose *Select All Text* from the drop-down menu.
3. In the top menu bar of Raritan Remote Console, click on **Serial**.
4. Choose *Copy* from the drop-down menu.
5. Position the cursor at the location you wish to paste the text and click once to make that location active.
6. In the top menu bar of Raritan Remote Console, click on **Serial**.
7. Select *Paste* from the drop-down menu.

Remote Desktop: Power Control

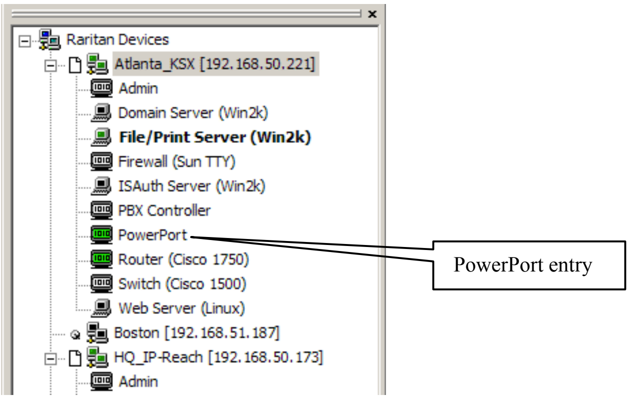
In addition to remote KVM and serial console access, Dominion KSX also offers users the option of graphical, hard power control. To take advantage of this capability, you should obtain and connect a Raritan remote power control unit to the dedicated “Power Control” port of Dominion KSX (see *Chapter 2: Installation*, “Physical Connections” for more details).

Raritan offers remote power control units in 1U and 0U form factors; offering 8, 12, or 20 outlets; and in configurations for different voltage, international, and load (amp rating) environments. Contact your Raritan representative for more information about Raritan remote power control units.

Please note that both the dedicated “Power Control” port and the graphical power control interface described below, only apply and operate with Raritan brand remote power control units. Similar devices from third party vendors will not function as described below with the dedicated “Power Control” port on Dominion KSX, however they of course can be connected to the Dominion KSX serial console ports – just as any other serial device.

Remote Connection

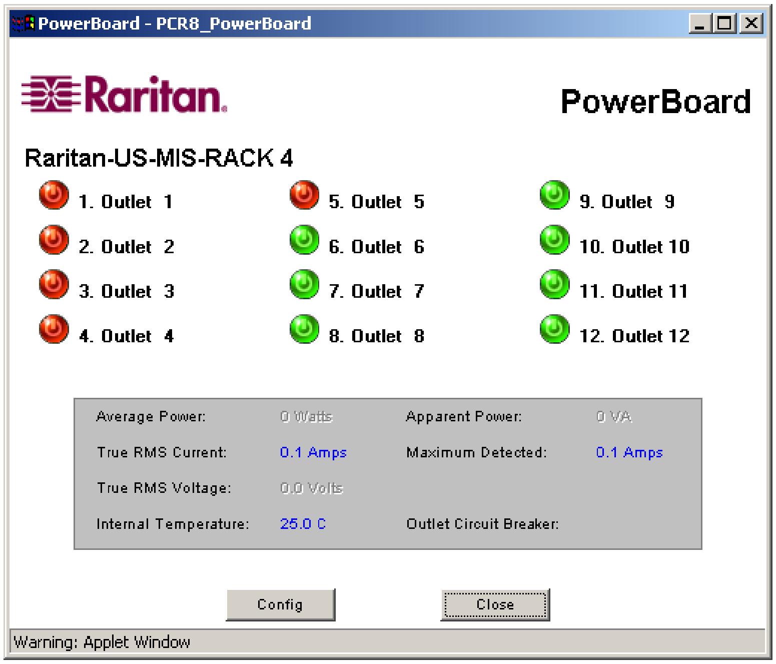
To open a remote connection to initiate remote power control, double-click on the corresponding Navigator entry named “PowerPort”, as displayed by RRC:



A window displaying the graphical power control interface (called “PowerBoard”), will appear, and the icon found next to the serial port entry on the RRC Navigator will turn green.

***Note**: If using Windows XP, Service Pack 1, the graphical power control interface will not appear if you have two conflicting Java virtual machines installed on your system (i.e., one from Sun Microsystems, and on from Microsoft).*

When the PowerBoard graphical power control interface appears, the user interface allows you to turn an outlet **ON** or **OFF** by clicking the icon before the Outlet name or number.



PowerBoard - PCR8_PowerBoard

Raritan. PowerBoard

Raritan-US-MIS-RACK 4

🟥 1. Outlet 1
🟥 2. Outlet 2
🟥 3. Outlet 3
🟥 4. Outlet 4
🟥 5. Outlet 5
🟩 6. Outlet 6
🟩 7. Outlet 7
🟩 8. Outlet 8
🟩 9. Outlet 9
🟩 10. Outlet 10
🟩 11. Outlet 11
🟩 12. Outlet 12

Average Power: 0 Watts
Apparent Power: 0 VA
True RMS Current: 0.1 Amps
Maximum Detected: 0.1 Amps
True RMS Voltage: 0.0 Volts
Internal Temperature: 25.0 C
Outlet Circuit Breaker:

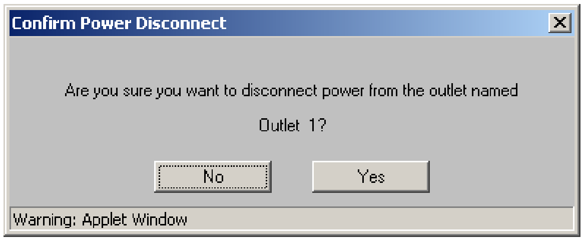
Warning: Applet Window

To Turn ON a Device or Outlet:

Whether or not a device is connected to an outlet, a **RED** icon before the outlet number indicates the outlet is OFF and there is no power feeding to it. Click on the red button icon, it will change to **GREEN**, indicating the outlet is now ON and there is power feeding to it.

To Turn OFF a Device or Outlet:

If the button icon before an outlet number is **GREEN**, click on the green button icon to turn OFF the outlet. A confirmation message will appear:



Confirm Power Disconnect

Are you sure you want to disconnect power from the outlet named

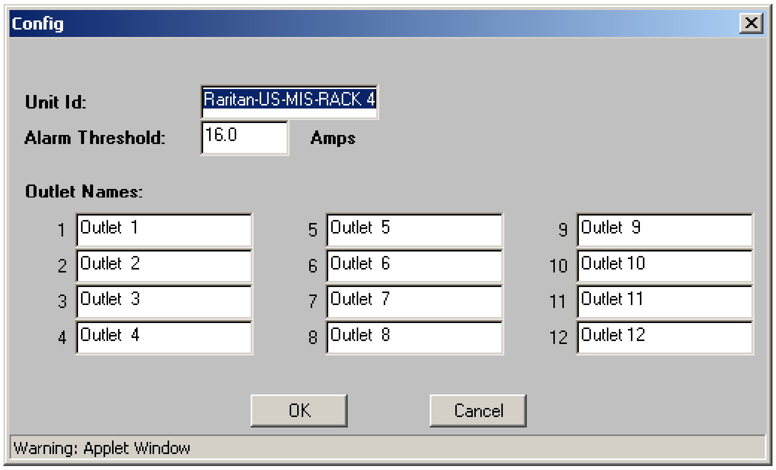
Outlet 1?

Warning: Applet Window

Click on the [**Yes**] button to turn off the outlet. The button icon for that outlet turns **RED** to indicate that the outlet is now OFF.

Configuration Options:

Click on the [**Config**] button the PowerBoard window to configure outlets on the power control unit. The Config window will appear.



Unit Id: Raritan-US-MIS-RACK 4

Alarm Threshold: 16.0 Amps

Outlet Names:

1	Outlet 1	5	Outlet 5	9	Outlet 9
2	Outlet 2	6	Outlet 6	10	Outlet 10
3	Outlet 3	7	Outlet 7	11	Outlet 11
4	Outlet 4	8	Outlet 8	12	Outlet 12

Options for Outlet configuration include:

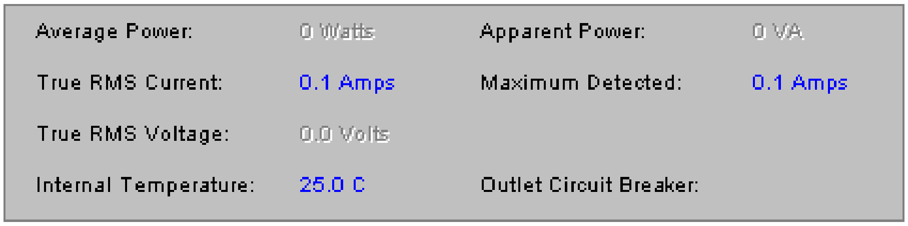
1. Assign a **Unit ID**: Give the power control unit an identification name, for example, using City, Building, Rack, or other information. *For example:* Raritan-US-MIS-RACK 4.
2. Set the **Alarm Threshold**, in Amps: When the threshold is reached, an audible alarm is activated to users located next to the power control unit.
3. Assign outlets specific **Outlet Names**: For easier identification and control, give each outlet a name.

Click on the [**OK**] button when finished to close the Configuration window and launch the PowerBoard Applet.

For your convenience, PowerBoard parameters are listed in the gray box in the PowerBoard window. These parameters are details that apply to the entire bank of outlets, and not on a per-outlet level.

Parameters include:

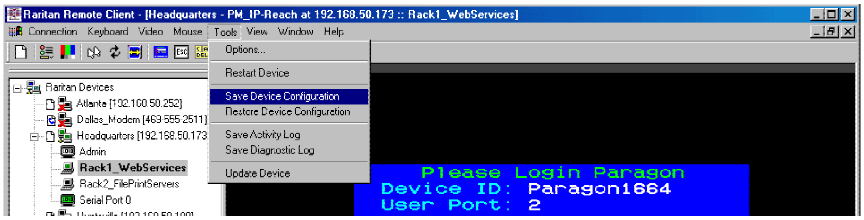
- Average power
- True RMS Current
- True RMS Voltage
- Internal Temperature
- Apparent Power
- Maximum Detected
- Outlet Circuit Breaker



Average Power:	0 Watts	Apparent Power:	0 VA
True RMS Current:	0.1 Amps	Maximum Detected:	0.1 Amps
True RMS Voltage:	0.0 Volts		
Internal Temperature:	25.0 C	Outlet Circuit Breaker:	

Remote Dominion KSX Device Administration

When logged into a Dominion KSX unit as a user with administrative privileges, Dominion KSX allows you to perform many powerful device administration tasks remotely.



Please Login Paragon
Device ID: Paragon1664
User Port: 2

Configuration Menus

An Administrative user can access Dominion KSX's lowest level configuration menus (explained in detail in **Chapter 4**), by double-clicking the "Admin" port entry of a Dominion KSX device shown in the RRC Navigator.

Firmware Upgrade

Remote firmware upgrades may be performed by selecting **Tools → Update Device** on the RRC Menu Bar. RRC will prompt you to locate a Raritan firmware distribution file (*.RFP format), which can be found on the Raritan web site (www.raritan.com) when available. Be sure to read all instructions included in firmware distributions before performing an upgrade.

Device Restart

Administrative users may restart Dominion KSX units by selecting **Tools → Restart Device** on the RRC Menu Bar.

Device Configuration Backup and Restore

By selecting **Tools → Save Device Configuration** and **Tools → Restore Device Configuration** on the RRC Menu Bar, Administrative users may download and upload complete Dominion KSX configurations to their local computers for archiving.

Log Files

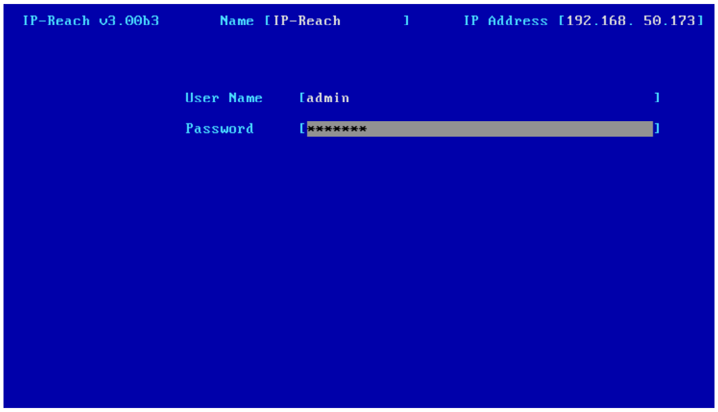
Dominion KSX provides detailed activity logs for troubleshooting purposes, which may be downloaded to your local computer for viewing, reporting, and analysis. On the RRC Menu Bar, select **Tools → Save Activity Log**, or **Tools → Save Diagnostic Log**.

Chapter 4: Administrative Functions

Accessing the Administrative Functions

Administrative functions may be accessed via the local admin console (see **Chapter 2: Installation, *Physical Connections***), or via remote administration (see **Chapter 3: Raritan Remote Client, *Remote Device Administration***). Only administrators (users with administrative privileges) can access the Dominion KSX Administrative Menus.

Local Admin Console



```
IP-Reach v3.00b3        Name [IP-Reach       ]       IP Address [192.168. 50.173]


                     User Name     [admin                                   ]
                     Password      [********                                ]
```

Power ON the Dominion KSX unit via the power switch on the back of the unit. The Administrative functions and menus will be displayed on the VGA monitor connected to your "Local Admin Console" ports, if connected as directed in **Chapter 2: Installation, *Physical Connections.***

Note: *The default Dominion KSX login user name is <admin>, with the password <raritan>. This user has administrative privileges.*
Passwords are case sensitive and must be entered in the exact case combination in which they were created. The default password <raritan> must be entered entirely in lowercase letters.
To ensure security, change the default username password as soon as possible.

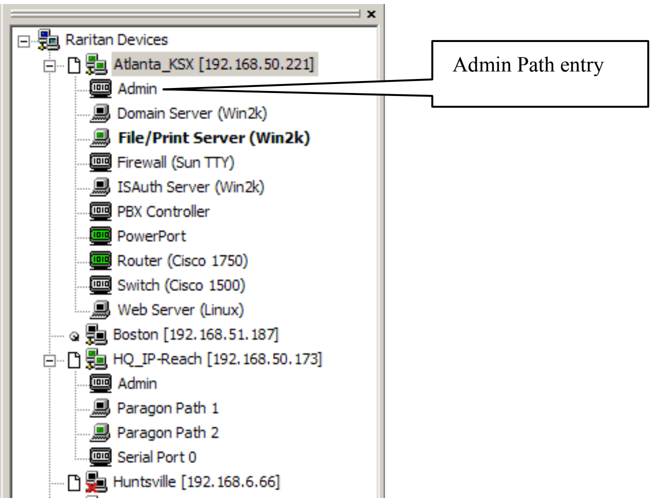
Remote Admin Console

An alternative way to access Dominion KSX's administrative functions is to do so remotely, using the Raritan Remote Client.

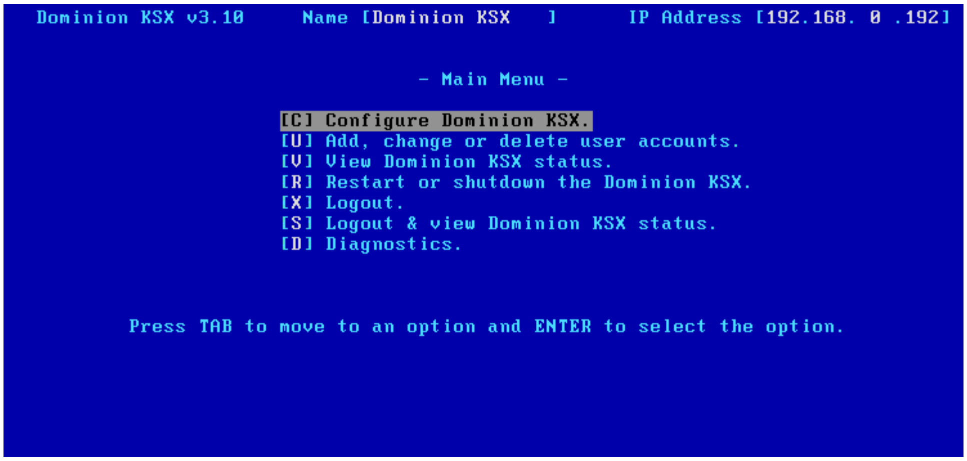
Any administrative user logged on to Dominion KSX can perform administrative functions remotely to make changes to the system, as long as Dominion KSX is set to allow remote administration privileges – see Allow Remote Administration on the Security Configuration screen.

***Note**: Only users with administrator privileges can access the Remote Admin feature.*

To access the Administrative menus from Raritan Remote Client, double click on the Admin path entry displayed on the RRC Navigator for the Dominion KSX unit you wish to configure.



Navigating the Administrative Menus

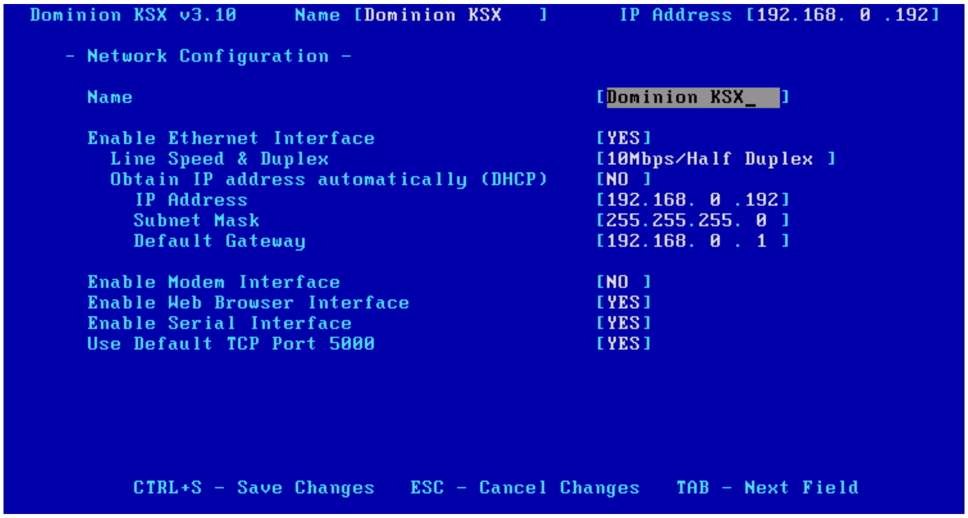


```
 Dominion KSX v3.10     Name [Dominion KSX   ]     IP Address [192.168. 0 .192]


                              - Main Menu -

                        [C] Configure Dominion KSX.
                        [U] Add, change or delete user accounts.
                        [V] View Dominion KSX status.
                        [R] Restart or shutdown the Dominion KSX.
                        [X] Logout.
                        [S] Logout & view Dominion KSX status.
                        [D] Diagnostics.



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

- Use the <**Tab**>, <↑>, <↓>, or <**C**> keys to highlight the menu selection, then press the <**Enter**> key. You may need to reboot.
- Press <**Ctrl+S**> to save changes.

Network Configuration

After making changes to the Network Configuration, press <**Ctrl+S**> to save. You must reboot when all changes are complete in order to apply them.



```
Dominion KSX v3.10     Name [Dominion KSX    ]      IP Address [192.168. 0 .192]

    - Network Configuration -

      Name                                        [Dominion KSX_  ]

      Enable Ethernet Interface                   [YES]
        Line Speed & Duplex                       [10Mbps/Half Duplex ]
        Obtain IP address automatically (DHCP)    [NO ]
          IP Address                              [192.168. 0 .192]
          Subnet Mask                             [255.255.255. 0 ]
          Default Gateway                         [192.168. 0 . 1 ]

      Enable Modem Interface                      [NO ]
      Enable Web Browser Interface                [YES]
      Enable Serial Interface                     [YES]
      Use Default TCP Port 5000                   [YES]




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

- **Name:** Designate a unique name for this Dominion KSX unit, for example, "Miami Sales Office." The default name is Dominion KSX.
- **Enable Ethernet Interface:** Designates whether Dominion KSX should enable its Ethernet adapter as active (default: YES).

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

  – **Line Speed & Duplex:** Enter the network speed to be used by Dominion KSX's Ethernet interface: Auto detect, 10 Mbps/Full Duplex, 10 Mbps/Half Duplex, 100 Mbps/Full Duplex, or 100 Mbps/Half Duplex

  – **Obtain IP address automatically (DHCP):**

    ▪ **YES**: Enables dynamic IP addressing for Dominion KSX. Each time Dominion KSX boots, it will request an IP address from the local DHCP server. Note that this setting can make remote access to Dominion KSX from outside the LAN difficult, since the dynamically assigned IP address must be known in order to initiate a connection.

    ▪ **NO** (default): Assigns a fixed IP address to the Dominion KSX unit (recommended).

      ✓ **IP Address**: Enter the IP address for Dominion KSX given by your Network Administrator.

      ✓ **Subnet Mask**: Enter a Subnet Mask provided by your Network Administrator.

      ✓ **Default Gateway**: Enter the Default Gateway if your Network Administrator specifies one.

- **Enable Modem Interface:** Enables Dial-up Modem access (default: YES).
- **Enable Web Browser Interface**: Enables web browser access to Dominion KSX (default: YES).
- **Enable Serial Interface**: Enables remote access to the serial devices connected to Dominion KSX's Serial IN port (default: YES).
- **Use Default TCP Port 5000**:

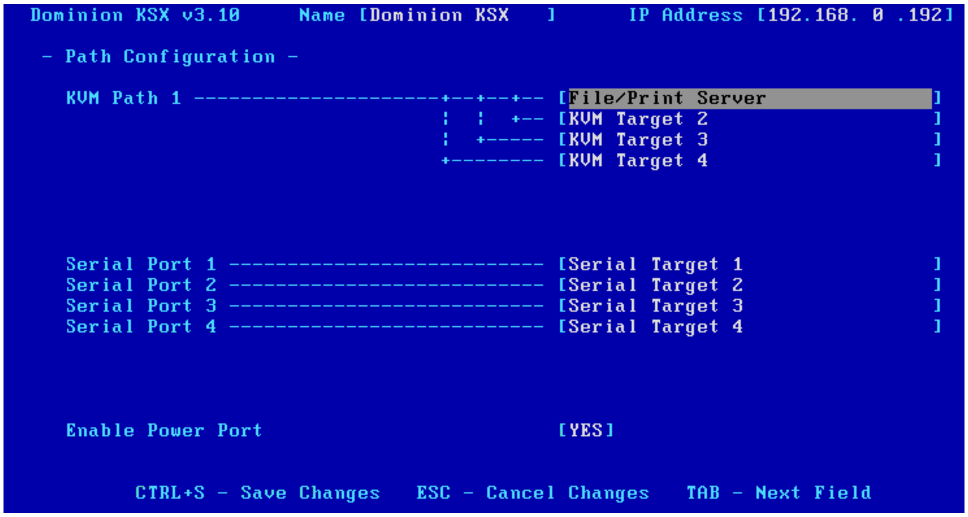
  – **YES (default):** Utilizes the default port 5000.

  – **NO:** Enter an alternate port number.

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

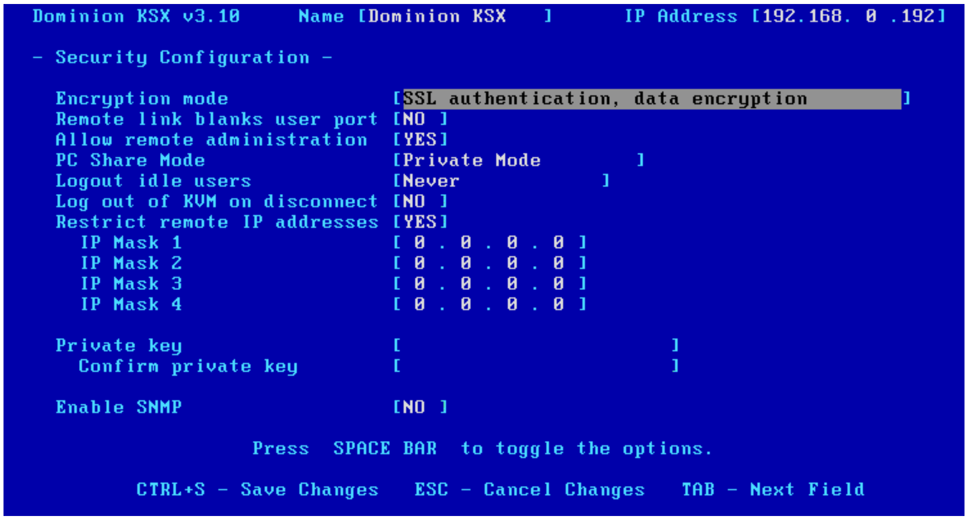
Path Configuration

On the Main Menu, select **Configuration → Path Configuration** to name each KVM Input and Serial Input port. Ports will be displayed alphabetically. The unit must be restarted in order for these configurations to take effect.



```
 Dominion KSX v3.10     Name [Dominion KSX    ]      IP Address [192.168. 0 .192]

  - Path Configuration -

    KVM Path 1 ---------------------+--+--+-- [File/Print Server              ]
                                    |  |  +-- [KVM Target 2                   ]
                                    |  +----- [KVM Target 3                   ]
                                    +-------- [KVM Target 4                   ]



    Serial Port 1 --------------------------- [Serial Target 1                ]
    Serial Port 2 --------------------------- [Serial Target 2                ]
    Serial Port 3 --------------------------- [Serial Target 3                ]
    Serial Port 4 --------------------------- [Serial Target 4                ]



    Enable Power Port                         [YES]


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

Security Configuration



```
 Dominion KSX v3.10     Name [Dominion KSX    ]      IP Address [192.168. 0 .192]

  - Security Configuration -

    Encryption mode              [SSL authentication, data encryption     ]
    Remote link blanks user port [NO ]
    Allow remote administration  [YES]
    PC Share Mode                [Private Mode         ]
    Logout idle users            [Never             ]
    Log out of KVM on disconnect [NO ]
    Restrict remote IP addresses [YES]
      IP Mask 1                  [ 0 . 0 . 0 . 0 ]
      IP Mask 2                  [ 0 . 0 . 0 . 0 ]
      IP Mask 3                  [ 0 . 0 . 0 . 0 ]
      IP Mask 4                  [ 0 . 0 . 0 . 0 ]

    Private key                  [                       ]
      Confirm private key        [                       ]

    Enable SNMP                  [NO ]

                     Press  SPACE BAR  to toggle the options.

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

- **Encryption mode:** Toggle through the choices and select the desired level of encryption for initial connection authentication and remote session video data transfer.
  - **No encryption**: No encryption or security. Neither the initial connection authentication nor remote video data transfer is encrypted.
  - **SSL authentication, NO data encryption:** This mode secures user names and passwords, but not KVM data. 128-bit Secure Socket Layer (SSL) protocol provides a private communications channel between Dominion KSX and the Remote PC during initial connection authentication. No encryption security in place during remote KVM data transfer.
  - **SSL authentication, data encryption (default):** This mode secures user names, passwords, and KVM data. 128-bit Secure Sockets Layer (SSL) protocol provides a private communications channel between Dominion KSX and the Remote PC during initial connection authentication. After authentication, KVM data is also transferred with 128-bit encryption, but using a proprietary protocol more efficient than SSL.

  - **SSL authentication, SSL data encryption:** This mode 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 Dominion KSX and the Remote PC during initial connection authentication. 128-bit SSL encryption is also in place during remote KVM data transfer.

> ***Note:*** *SSL data encryption increases the amount of data that must be sent over the remote connection, and is, therefore, not recommended for modem or very slow Internet connections. The default setting "SSL authentication, data encryption" offers exactly the same level of security with a higher level of efficiency.*

- **Remote link blanks user port:** Determines whether the Direct Analog User port will be blanked out locally when a remote user is accessing the corresponding KVM port. This keeps a local user from seeing what the remote user is doing.
  - **NO (default):** User port can be viewed locally during remote user access.
  - **YES:** User port cannot be viewed locally during remote user access. The local or Direct Analog user console will stop displaying video.
- Allow remote administration:
  - **NO:** To keep access to all Administrative Functions available only from the Dominion KSX Admin Console, and not from a Remote PC.
  - **YES (default):** Allows remote access to all Administrative Dominion KSX Functions by administrators logged on at a Remote PC. See 9. Remote Administration.
- **PC Share Mode:** Determines global concurrent remote access. Enables up to eight remote users to simultaneously log on to one Dominion KSX unit and concurrently view and control the same Target KVM Server through Dominion KSX. Control is based on first active/keyboard mouse input, so multiple remote users attempting keyboard input or mouse movement at exactly the same moment may experience uneven control.
  - **Private Mode (default):** No PC Share. Each Dominion KSX path can be accessed exclusively by only one user at a time.
  - **PC Share Mode:** Dominion KSX ports can be accessed by more than one user (administrator or non-administrator) at a time. Control is based on first active keyboard/mouse input, so multiple remote users attempting keyboard input or mouse movement at exactly the same moment may experience uneven control.
  - **PC Share Admins Only:** Dominion KSX can be accessed by more than one user (administrative users only) at a time. Control is based on first active keyboard/mouse input, so multiple remote users attempting keyboard input or mouse movement at exactly the same moment may experience uneven control.

> ***Note:*** *PC Share Mode is a global setting. For individual user access settings see Keyboard and Mouse Control and Concurrent Access Mode on the User Account Settings screen. Each user profile can be set individually to enable/disable keyboard and mouse control, and concurrent access.*

- **Logout idle users:** Offers an option for Dominion KSX to automatically disconnect remote users after certain selected time intervals of inactivity have passed.
  - **Never** (default): Idle remote users will never be disconnected.
  - **After 5, 15, 30, 60, or 120 minutes**: Idle remote users will be automatically disconnected from Dominion KSX after the selected time period has passed with no active input from the Remote PC.
- **Restrict remote IP address:** Determines which remote IP address locations will be granted access to Dominion KSX.
  - **NO (default):** Remote access to Dominion KSX is unrestricted.
  - **YES:** Dominion KSX will grant remote access to up to four designated IP addresses or address levels. Administrators can set Dominion KSX to accept requests only from the company's intranet and/or from just a few outside IP addresses. The IP Mask fields determine what remote IP addresses Dominion KSX will grant remote access to.
    - A specific IP Mask instructs Dominion KSX to grant remote access only to this specific remote IP address. For example, a mask of 10.0.0.1 instructs Dominion KSX to grant remote access from the remote IP address location 10.0.0.1 only.
    - The value 255 acts as a wildcard in any location of the IP mask address. For example, a mask of 10.0.0.255 instructs Dominion KSX to grant remote access from any remote IP address location within the range 10.0.0.0 to 10.0.0.255. Similarly, a mask of 192.255.255.255 instructs Dominion KSX to grant remote access from any remote IP address location beginning with 192.

Note: *Once Restrict remote IP address has been enabled, an entry must be made in at least one of the IP Mask fields, since 0.0.0.0 is an invalid IP address.*

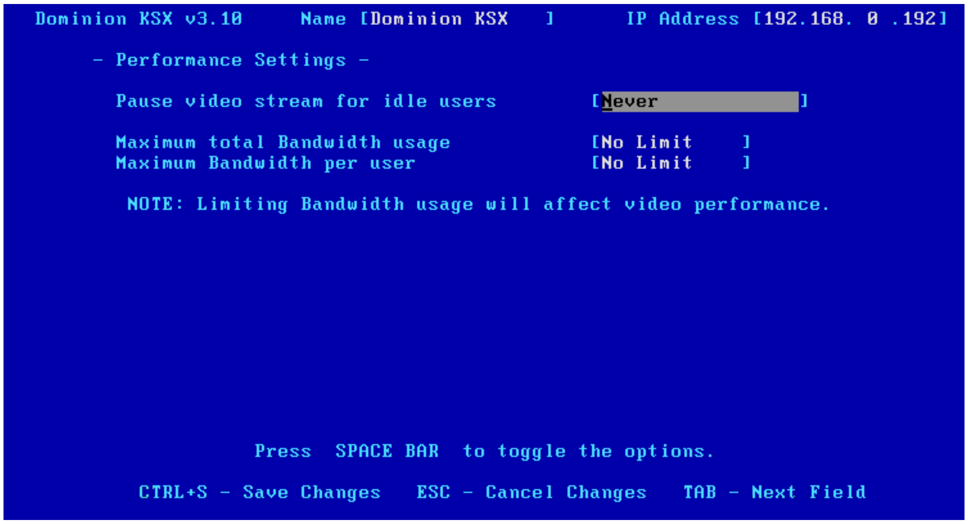
- **Private key**: Enter a private key password. This private key acts as a second level of password protection. Only remote users who know the private key password, in addition to their user name and password, can log in and connect to Dominion KSX.
  - **Confirm private key:** Enter private key password again for re-confirmation.

Note: *Private key passwords are case sensitive. For remote user login, passwords must be entered by the user in the exact case combination in which they were created here.*

Note: *Private key passwords must be alphanumeric. Special characters cannot be used.*

Performance Settings

The Performance Settings screen is used to set up Dominion KSX's video data transfer and bandwidth parameters.



```
Dominion KSX v3.10     Name [Dominion KSX    ]      IP Address [192.168. 0 .192]

     - Performance Settings -

       Pause video stream for idle users         [Never             ]

       Maximum total Bandwidth usage             [No Limit     ]
       Maximum Bandwidth per user                [No Limit     ]

        NOTE: Limiting Bandwidth usage will affect video performance.

                    Press  SPACE BAR  to toggle the options.

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

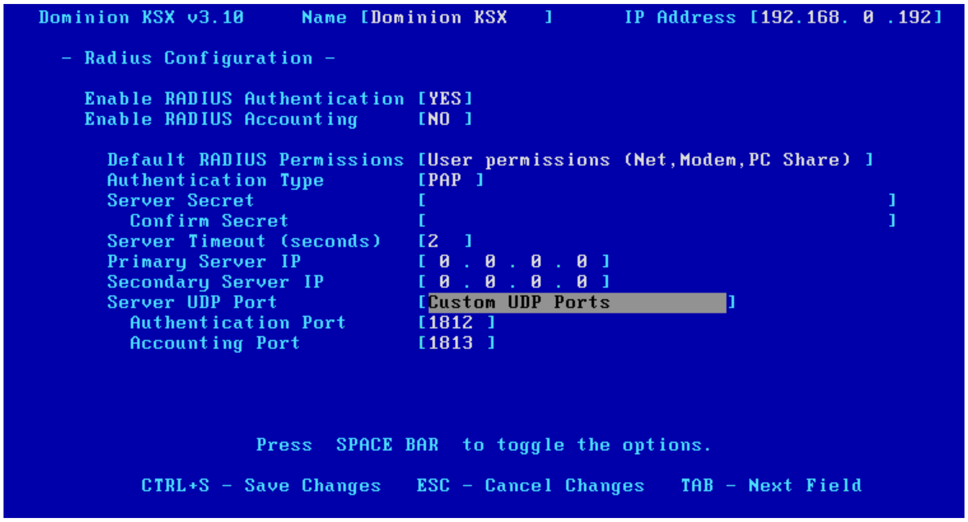
- **Pause video stream for idle users**: Pausing the flow of video data during periods of prolonged inactivity will prevent an inactive user from needlessly consuming bandwidth.
  - **Never (default):** Video data will continually be sent to Remote PC, constantly updating the screen, even if the remote user is Idle, sending no active input to Dominion KSX.
  - **After 5, 15, 30, 60, or 120 minutes:** Video data flow to the Remote PC will pause after the selected time period has passed with no active input from the Remote PC.
- **Maximum total Bandwidth usage**: Sets an upper limit to the amount of bandwidth that can be consumed by this one Dominion KSX unit.
  - **No Limit (default):** Dominion KSX can consume as much bandwidth as needed.
  - **10, 5, 2, or 1 megabit or 512, 256, 128 kilobit**: Total bandwidth available to be consumed by this Dominion KSX **unit** is limited to the selected quantity. The lower the bandwidth allowed, the slower the performance that may result.
- **Maximum Bandwidth per user**: Sets an upper limit to the amount of bandwidth that can be consumed by each user logged onto this one Dominion KSX unit.
  - **No Limit (default):** Each **active** user can consume as much bandwidth as needed.
  - **10, 5, 2, or 1 megabit or 512, 256, 128 kilobit:** Bandwidth consumed by each active user during the **operation** of this Dominion KSX unit is limited to the selected quantity. The lower the bandwidth allowed, the slower the performance that may result.

Press <**Ctrl+S**> to save changes or <**Esc**> to cancel changes, and return to Configuration Menu. Saved Performance Settings changes will not take effect until Dominion KSX is restarted.

RADIUS Configuration

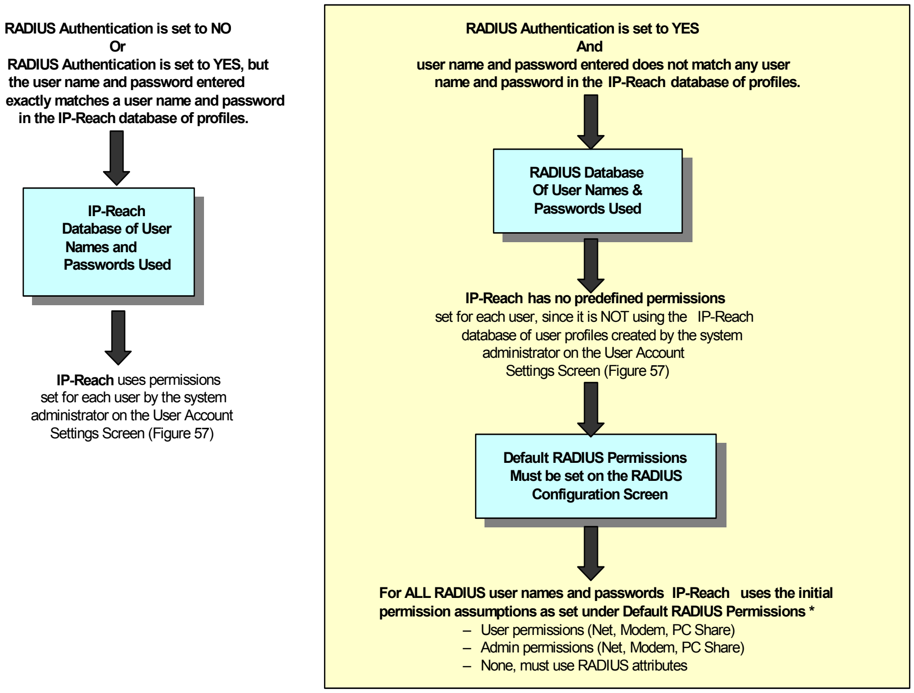
The Radius Configuration screen is used to set up Dominion KSX for use with a RADIUS protocol server. RADIUS protocol is an Internet standard that provides user authentication, authorization, and accounting services for remote access devices. Dominion KSX can be configured as a RADIUS client, and will query the RADIUS server for authentication and authorization information each time a user attempts to log on to Dominion KSX. Dominion KSX can also send information about when each user logged in or out to the RADIUS accounting server.

Please be sure to carefully review **Appendix C: RADIUS Server Settings** to understand the details regarding Dominion KSX's RADIUS implementation.



```
 Dominion KSX v3.10     Name [Dominion KSX    ]      IP Address [192.168. 0 .192]

   - Radius Configuration -

     Enable RADIUS Authentication [YES]
     Enable RADIUS Accounting     [NO ]

       Default RADIUS Permissions [User permissions (Net,Modem,PC Share) ]
       Authentication Type        [PAP ]
       Server Secret              [                                       ]
         Confirm Secret           [                                       ]
       Server Timeout (seconds)   [2  ]
       Primary Server IP          [ 0 . 0 . 0 . 0 ]
       Secondary Server IP        [ 0 . 0 . 0 . 0 ]
       Server UDP Port            [Custom UDP Ports           ]
         Authentication Port      [1812 ]
         Accounting Port          [1813 ]



                      Press  SPACE BAR  to toggle the options.

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

- **Enable RADIUS Authentication**: Turns the RADIUS authentication function on or off.
  - **NO (default):** RADIUS authentication is not operational. At a user login attempt, Dominion KSX will refer to the Dominion KSX database of user name and password profiles that have been entered and built by the system administrator.
  - **YES:** RADIUS authentication is operational. At a user login attempt, Dominion KSX will refer to the RADIUS server's user name and password database, provided there is not an exact matching user name and password in the Dominion KSX database of profiles.


RADIUS Authentication is set to NO
Or
RADIUS Authentication is set to YES, but the user name and password entered exactly matches a user name and password in the IP-Reach database of profiles.
IP-Reach Database of User Names and Passwords Used
IP-Reach uses permissions set for each user by the system administrator on the User Account Settings Screen (Figure 57)
RADIUS Authentication is set to YES
And
user name and password entered does not match any user name and password in the IP-Reach database of profiles.
RADIUS Database Of User Names & Passwords Used
IP-Reach has no predefined permissions set for each user, since it is NOT using the IP-Reach database of user profiles created by the system administrator on the User Account Settings Screen (Figure 57)
Default RADIUS Permissions Must be set on the RADIUS Configuration Screen
For ALL RADIUS user names and passwords IP-Reach uses the initial permission assumptions as set under Default RADIUS Permissions *
– User permissions (Net, Modem, PC Share)
– Admin permissions (Net, Modem, PC Share)
– None, must use RADIUS attributes

- **Default RADIUS Permissions**: With RADIUS Authentication operational, “Default RADIUS Permissions” defines the basic initial permissions or privileges for all RADIUS user name and password profiles.

> ***Note:*** *These initial RADIUS permissions can be changed for each individual user, by overriding attributes returned by the RADIUS server. Please see* ***Appendix B: RADIUS Server Settings*** for more information**.**

  – **User permissions (Net, Modem, PC Share) (Default):** All RADIUS authenticated users will have user level (non administrative) access to Dominion KSX over the network and via modem. All users will also have PC Share power, giving them concurrent access capability. That means they can connect to a Dominion KSX KVM port even if another user is already connected. Keyboard and mouse control is also granted.

  – **Admin permissions (Net, Modem, PC Share):** All RADIUS authenticated users will have Administrator level (with Admin powers) access to Dominion KSX over the network or via modem. All users will also have PC Share power, giving them concurrent access capability. That means they can connect to a Dominion KSX KVM port even if another user is already connected. Keyboard and mouse control is also granted.

> ***Note:*** *Control during concurrent access to a Target KVM Server in PC Share mode will be based on first active keyboard/mouse input, so multiple remote users attempting keyboard input or mouse movement at exactly the same moment may experience uneven control. RADIUS users with individual PC Share capability will only be able to connect concurrently to Dominion KSX provided the global PC Share Mode setting on the Security Configuration screen also enables it.*

  – **None, must use RADIUS attributes:** No assumed initial permissions exist. All RADIUS authenticated users will be denied access to Dominion KSX unless they are given specific permission to gain access. Specific permission takes the form of FILTER-ID attributes, which are returned by the RADIUS server for each individual RADIUS user. See Appendix C for details regarding Filter ID attributes.

- **Authentication Type**: Controls which password authentication protocol will be used between Dominion KSX Control on the Remote PC, Dominion KSX, and the RADIUS server.

  – **PAP (Default):** Password Authentication Protocol (PAP) will be used to encrypt and authenticate the user’s password.

> ***Note:*** *PAP is slightly less secure than CHAP, but some RADIUS servers require the PAP protocol.*

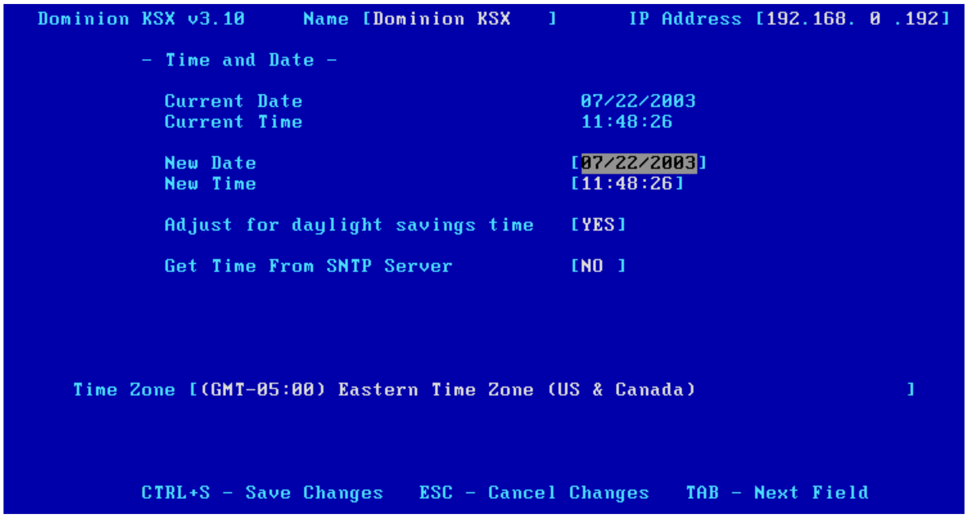
  - **CHAP:** Challenge Authentication Protocol (CHAP) will be used to encrypt and authenticate the user's password.
- **Server Secret**: The RADIUS server and Dominion KSX, as a RADIUS client, share a common secret used to encrypt the RADIUS protocol data. Enter the secret here. The keystrokes entered for the secret can be any combination of keystrokes up to 128 characters in length.
  - **Confirm Secret:** Enter secret again for confirmation of keystrokes.
- **Primary Server IP:** Enter the IP address of the primary RADIUS server. A primary server IP is required for the RADIUS features to function.
- **Secondary Server IP:** Optional. Enter the IP address of a secondary RADIUS server. If the primary server becomes unavailable, Dominion KSX will redirect its RADIUS requests to this secondary or backup server.
- **Server UDP Port:** Sets the ports used by the RADIUS server.
  - **Standard 1812 & 1813 (default):** Uses port 1812 for Authentication and port 1813 for Accounting. These are the ports most often used by modern RADIUS systems.
  - **Legacy Ports 1645 & 1646:** Uses port 1645 for Authentication and port 1646 for Accounting. These ports are most often used by older RADIUS systems.
  - **Custom UDP Ports:** Enables the administrator to enter specific port numbers for the RADIUS server.
    - **Authentication Port:** Enter port number used by RADIUS for Authentication.
    - **Accounting Port:** Enter the port number used by RADIUS for Accounting.
- **Enable RADIUS Accounting:** Turns the RADIUS accounting function on or off.
  - **NO (default):** RADIUS accounting is operational. Log in and log out information for each user will be recorded only in Dominion KSX's built-in event log.
  - **YES:** RADIUS accounting is operational. Log in and log out information for each user will be recorded in Dominion KSX's built-in event log, and then Dominion KSX will send a RADIUS accounting message to the RADIUS server.

Note: *If RADIUS Authentication has been enabled, the choices previously made for Secret Server, Confirm Secret, Primary Server IP, and Secondary Server IP will also accommodate RADIUS Accounting. If these selections have not been made during a previous enabling of RADIUS Authentication, they must now be selected for RADIUS Accounting.*

Press <**Ctrl+S**> to save changes or <**Esc**> to cancel changes, and return to the Configuration Menu. Saved Radius Configuration changes will not take effect until Dominion KSX is restarted.

Time and Date

Current Date and Time on the Dominion KSX unit are listed on this screen. Once saved, Time and Date changes will not take effect until Dominion KSX is restarted.



```
  Dominion KSX v3.10     Name [Dominion KSX   ]      IP Address [192.168. 0 .192]

            - Time and Date -

              Current Date                           07/22/2003
              Current Time                           11:48:26

              New Date                              [07/22/2003]
              New Time                              [11:48:26]

              Adjust for daylight savings time      [YES]

              Get Time From SNTP Server             [NO ]



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


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

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

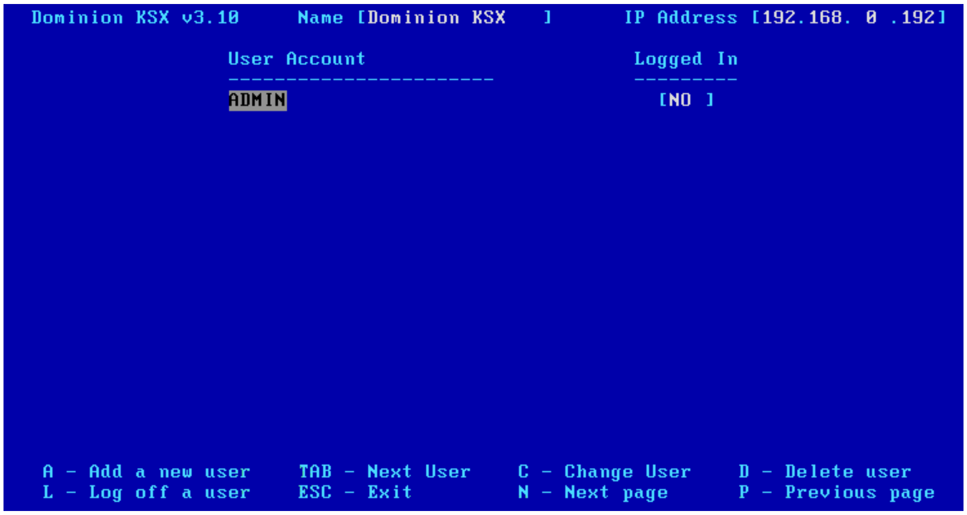
Press <**Ctrl+S**> to save changes or <**Esc**> to cancel changes, and return to the Configuration Menu. Saved Radius Configuration changes will not take effect until Dominion KSX is restarted.

Key Configuration

Select [**K**] to add Dominion KSX User License Key codes, increasing the total number of usernames that can be entered into the Dominion KSX system.

Administer User Accounts

The Add, Change, or Delete User Accounts screen lists all existing user accounts for Dominion KSX and shows if each user is currently logged in to Dominion KSX from a Remote PC. Administrators who log on to the Dominion KSX Admin Console can use this screen to administer Dominion KSX user accounts.



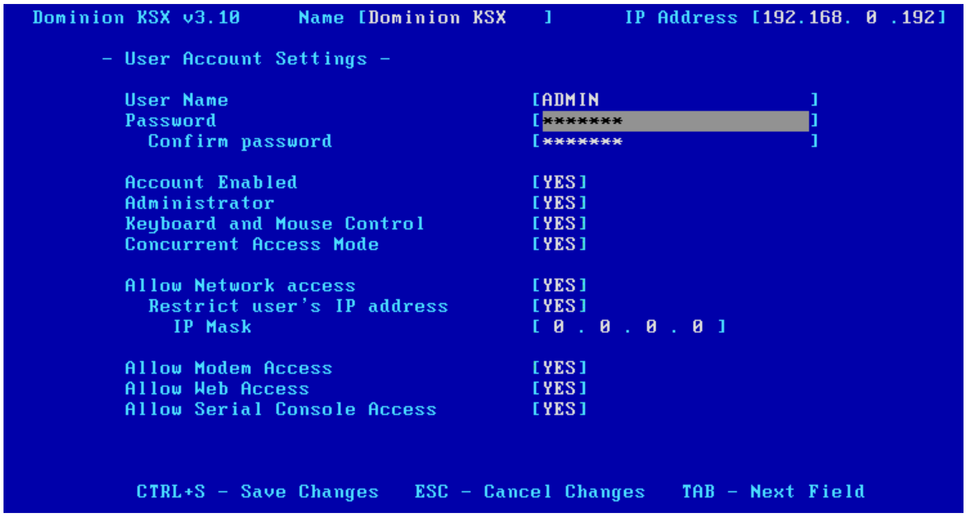
```
 Dominion KSX v3.10     Name [Dominion KSX    ]      IP Address [192.168. 0 .192]

                  User Account                       Logged In
                  -----------------------            ---------
                  ADMIN                                [NO ]




  A - Add a new user    TAB - Next User    C - Change User    D - Delete user
  L - Log off a user    ESC - Exit         N - Next page      P - Previous page
```

Add New Users

Press the letter <**A**> ('Add a new user') to access the User Account Settings screen and add a new user profile.

> ***Note:*** *Dominion KSX will limit the number of total users (not including ADMIN) that can be added to the database, depending on the number of user licenses purchased. Be sure to enter your user license key codes by selecting* ***[K] Key Configuration*** *in the Configuration menu.*

Use the <**Tab**>, <↑>, or <↓> keys to select each line on the User Account Settings screen and the <**space bar**> or the <←> or <→> keys to toggle between available entries. Press <**Enter**>, <**Tab**> or <↓> when your entry on each line is complete.



```
 Dominion KSX v3.10     Name [Dominion KSX    ]      IP Address [192.168. 0 .192]

        - User Account Settings -

          User Name                           [ADMIN                   ]
          Password                            [*******                 ]
            Confirm password                  [*******                 ]

          Account Enabled                     [YES]
          Administrator                       [YES]
          Keyboard and Mouse Control          [YES]
          Concurrent Access Mode              [YES]

          Allow Network access                [YES]
            Restrict user's IP address        [YES]
              IP Mask                         [ 0 . 0 . 0 . 0 ]

          Allow Modem Access                  [YES]
          Allow Web Access                    [YES]
          Allow Serial Console Access         [YES]


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

- **User Name:** Enter a new user name.
- **Password:** Enter a password to be associated with this user name.
  - **Confirm password:** Enter password again for confirmation of keystrokes.

Note: *Passwords are case sensitive. For user login, passwords must be entered by the user in the exact case combination in which they were created here. User names and passwords entered in this Dominion KSX user profile database each have a 24-character limit. RADIUS user names and passwords can each be up to 128 characters.*

- **Account Enabled**:
  - **YES (default):** Permits this user name and profile to be actively used to gain access to Dominion KSX.
  - **NO:** The saved user profile will exist, but cannot be actively used to log in to Dominion KSX.
- **Administrator:**
  - **NO (default):** The user name being profiled will not have Administrator privileges.
  - **YES:** This user will have Administrator privileges and powers.
- **Keyboard and Mouse Control:** Determines whether user has keyboard and mouse control during a remote KVM connection.
  - **YES (default):** Grants the user keyboard and mouse control.
  - **NO:** User will not have keyboard and mouse control during a remote connection.

Note: *The Keyboard and Mouse Control setting chosen determines whether the next setting for Concurrent Access Mode, if activated, will result in PC Share or Public view.*

- **Concurrent Access Mode:** Determines each individual user's ability to remotely log on to a Dominion KSX KVM Port when another user has already established a remote connection.
  - **YES (default):** User can log on to a Dominion KSX KVM Port and establish a remote connection when another user has already established a remote connection to that same port. The status of this sharing depends upon the user's prior setting for Keyboard and Mouse Control.
    - *If Keyboard and Mouse Control = YES:* Sharing is in PC Share mode, concurrent access by more than one user. However, control will be based on first active keyboard/mouse input for all users with Keyboard and Mouse Control, so multiple remote users attempting keyboard input or mouse movement at exactly the same moment may experience uneven control.
    - *If Keyboard and Mouse Control = NO:* Sharing is in Public View mode, concurrent access by more than one user, but each user with NO Keyboard and Mouse Control can only view the video and has no control.
  - **NO:** This user can log on to a Dominion KSX KVM Port and establish a remote connection only if no other user is currently logged onto a KVM Port already.

Note: *Concurrent Access Mode is an individual user setting. For global access settings see PC Share Mode on the Security Configuration screen.*

- **Allow Network access:** Determines whether this user will be able to access Dominion KSX via a Network connection for LAN/WAN or Internet access.
  - **YES (default):** The user will have Network connection capability.
    - **Restrict user's IP address:** Determines whether this user's remote network access will be limited to a particular remote IP address location or level.
      - ✓ **NO (default):** The user has remote network access to Dominion KSX from any remote IP address location.
      - ✓ **YES:** The user's network access to Dominion KSX will be limited to a network connection originating from a designated remote IP address location or remote IP address level.

Note: *Once Restrict user's IP address has been enabled, an entry must be made in at least one of the IP Mask fields, since 0.0.0.0 is an impossible IP address.*

  - **IP Mask:** Enter remote IP address location from which this user will be granted remote network access. A specific IP Mask instructs Dominion KSX to grant remote access to only this specific remote IP address. For example, a mask of 10.0.0.1 instructs Dominion KSX to grant remote access from the remote IP address location 10.0.0.1 only. The value 255 acts as a wildcard in any location of the IP mask address. For example, a mask of 10.0.0.255 instructs Dominion KSX to grant this user remote access from any remote IP address location within the range 10.0.0.0 to 10.0.0.255. Similarly, a mask of 192.255.255.255 instructs Dominion KSX to grant this user remote access from any remote IP address location beginning with 192.
  - **NO:** The user has no network connection capability.

- **Allow Modem Access:** Determines whether this user will be able to access Dominion KSX via a Modem connection for access via and analog telephone line.
  - **NO:** The user will not have Modem connection capability.
  - **YES (default):** The user will have Modem connection capability.

Press <**Ctrl+S**> to save changes or <**Esc**> to cancel changes, and return to the Add, Change, or Delete User Accounts screen.

Change User Profile

See the previous section ***Add New Users*** and the User Account Settings screen for details on setting user profile specifics. When you have made the required changes to the User Profile, press <**Ctrl+S**> to save changes or <**Esc**> to cancel changes, and return to the Add, Change, or Delete User Accounts screen.

Delete Users

Use the <**Tab**>, <↑>, or <↓> keys to select a user from the Add, Change, or Delete User Accounts screen and press the letter <**D**> to delete the user profile selected. Dominion KSX will ask you if you are sure that you want to delete this user.

- **Y**: Yes. The selected user will be deleted and Dominion KSX will return you to the Add, Change, or Delete User Accounts screen showing all user profiles, with the deleted user no longer listed.
- **N**: No. Dominion KSX will return you to the Add, Change, or Delete User Accounts screen, showing all user profiles, with the selected user still listed.

Log Off Users

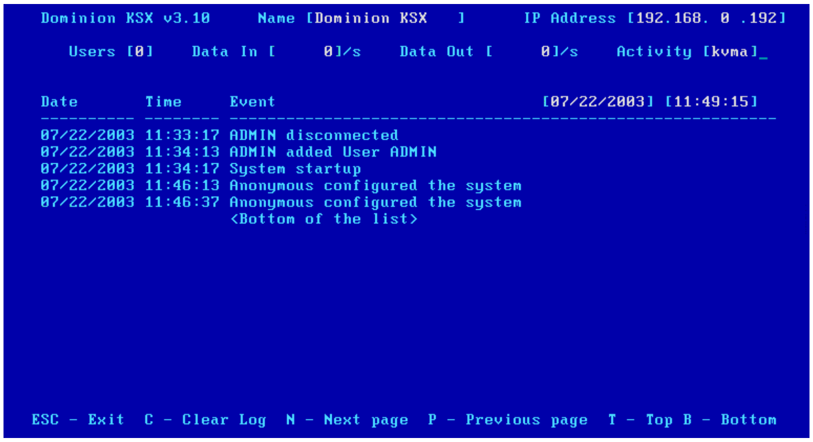
Use the <**Tab**>, <↑>, or <↓> keys to select a user from the Add, Change, or Delete User Accounts screen who is currently remotely logged in to Dominion KSX (**Logged in – YES**) and press the letter <**L**> to log off the selected user. Dominion KSX will ask you if you are sure that you want to log off this user.

- **Y**: Yes. The selected user will be logged off of Dominion KSX and the remote session will end. Dominion KSX will return you to the Add, Change, or Delete User Accounts screen, showing all user profiles, with the selected user no longer listed as logged in.
- **N**: No. Dominion KSX will return you to the Add, Change, or Delete User Accounts screen, showing all user profiles, with the selected user still listed as being logged in.

View Dominion KSX Status

The Dominion KSX Event Log screen shows a log file containing information about Dominion KSX log in and connection activities. This Event Log stores Dominion KSX events, such as user login or logout, bad login attempts, Admin login, and logout at the Dominion KSX Admin console, Admin changes to the system configuration, Admin user profile additions, changes, or deletions, modem activity, system startup and shutdown, and all errors that occur, with the date and time of each event. Please see **Appendix F: Troubleshooting** for a listing of error codes with their meaning and suggested solution. Up to 2,048 events can be stored in one log file.

Dominion KSX also auto-recovers from fatal errors. If a fatal error occurs, it is recorded and Dominion KSX automatically reboots. If a non-fatal error occurs, it is recorded and Dominion KSX waits until all users are logged off the system, and then it reboots to make sure the previous non-fatal error does not escalate to a fatal error.



```
  Dominion KSX v3.10     Name [Dominion KSX    ]      IP Address [192.168. 0 .192]

     Users [0]     Data In [      0]/s     Data Out [      0]/s     Activity [kvma]_

  Date       Time      Event                              [07/22/2003] [11:49:15]
  ---------- -------- ----------------------------------------------------------
  07/22/2003 11:33:17 ADMIN disconnected
  07/22/2003 11:34:13 ADMIN added User ADMIN
  07/22/2003 11:34:17 System startup
  07/22/2003 11:46:13 Anonymous configured the system
  07/22/2003 11:46:37 Anonymous configured the system
                      <Bottom of the list>










 ESC - Exit  C - Clear Log  N - Next page  P - Previous page  T - Top B - Bottom
```

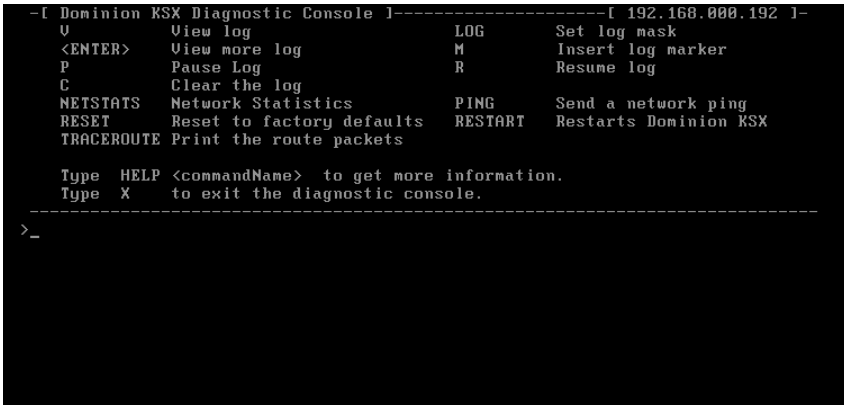
Restart or Shutdown the Dominion KSX

Offers options to **Restart** <**R**>, **Shutdown** <**S**>, or **Cancel** <**Esc**> the restart or shutdown command. <**R**> Restarts the Dominion KSX unit and brings the Dominion KSX Admin Console back to the Dominion KSX Initialization screen.

Diagnostics

While navigating the Main Menu of the Administrative Console, pressing **<D>** and **<Enter>** will invoke the Dominion KSX Diagnostic functions.

These functions are meant to enable Raritan Technical Support to assist you in the case of a problem with your Dominion KSX unit. Do not invoke these functions unless you are fully aware of their meanings and intended use. Please contact Raritan Technical Support should you require more information.



```
 -[ Dominion KSX Diagnostic Console ]---------------------[ 192.168.000.192 ]-
    V          View log                      LOG       Set log mask
    <ENTER>    View more log                 M         Insert log marker
    P          Pause Log                     R         Resume log
    C          Clear the log
    NETSTATS   Network Statistics            PING      Send a network ping
    RESET      Reset to factory defaults     RESTART   Restarts Dominion KSX
    TRACEROUTE Print the route packets

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

Appendix A: Specifications

ITEM	DIMENSIONS (WxDxH)	WEIGHT	POWER
KSX 440	1U full width, rack mountable: 17.33" (W) x 21.26" (D) x 1.75" (H) 440 mm (W) x 540 mm (D) x 44 mm (H)	24.2lbs. (11kg.)	110/220V auto-switching (50/60 Hz European)
KSX 880	1U full width, rack mountable: 17.33" (W) x 21.26" (D) x 1.75" (H) 440 mm (W) x 540 mm (D) x 44 mm (H)	24.2lbs. (11kg.)	110/220V auto-switching (50/60 Hz European)

Remote Connection

Network:	10BASE-T, 100BASE-TX Ethernet
Modem:	56K modem included
Protocols:	TCP/IP, UDP, SNMP, HTTP, HTTPS, RADIUS

Raritan Remote Client (RRC) Software

Operating System Requirements: Windows XP / NT* / ME / 2000 / 2003 with DirectX and Java Virtual Machine.

* NT support for some international keys are limited due to Micros

KVM Input

Keyboard: PS/2

Mouse: PS/2

Video: VGA

Supported Resolutions:

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

Appendix B: Serial Port Pin-Out Diagrams

In order to provide maximum port density and to enable simple UTP (Category 5) cabling, the serial parts found on Dominion KSX via compact RJ45 ports. However, no widely adopted industry-standard exists for sending serial data over RJ45 connections. For your reference, the serial pin-out employed by Dominion KSX is provided below.

Dominion KSX RJ45 Serial Pin-Out

RJ45 (FEMALE)	FUNCTION
1	RTS
2	DTR
3	TXD
4	GND
5	SG
6	RXD
7	DSR
8	CTS

SCSDB25F Nulling Serial Adapter Pin-Out

RJ45 (FEMALE)	DB25 (FEMALE)
1	5
2	6, 8
3	3
4	1
5	7
6	2
7	20
8	4

SCSDB25M Nulling Serial Adapter Pin-Out

RJ45 (FEMALE)	DB25 (MALE)
1	5
2	6, 8
3	3
4	1
5	7
6	2
7	20
8	4

SCSDB9F Nulling Serial Adapter Pin-Out

RJ45 (FEMALE)	DB9 (FEMALE)
1	8
2	1, 6
3	2
4	SHELL
5	5
6	3
7	4
8	7

SCSDB9M Nulling Serial Adapter Pin-Out

RJ45 (FEMALE)	DB9 (MALE)
1	8
2	1, 6
3	2
4	SHELL
5	5
6	3
7	4
8	7

Custom, Nulling RJ45 Cable

Like Dominion KSX, many newer devices also provide serial ports in RJ45 form. However, as noted above, each implementation is proprietary: not all serial ports using RJ45 connectors are alike!

Owners of hardware with RJ45 serial ports, who very familiar with network cabling, may be able to crimp their own UTP/Cat 5 cable such that no adapters are necessary to connect their device to Dominion KSX; a single, custom-made UTP/Cat 5 cable can connect the device's RJ45 serial port to Dominion KSX's RJ45 serial device ports.

To do so, reference the RJ45 pin-out diagram above, along with the serial RJ45 pin-out diagram of your device.

CRLVR-15 Custom Rollover Cable for Most Sun / Cisco RJ45 Serial Ports

For your convenience, Raritan also provides P/N CRLVR-15, a custom Cat5 cable that enables most Sun / Cisco RJ45 serial ports to be connected directly to Dominion KSX serial ports. Alternatively, you may crimp this cable yourself by following the cable pin-out diagram below:

RJ45 (MALE)	RJ45 (MALE)
1	8
2	7
3	6
4	5
5	4
6	3
7	2
8	1

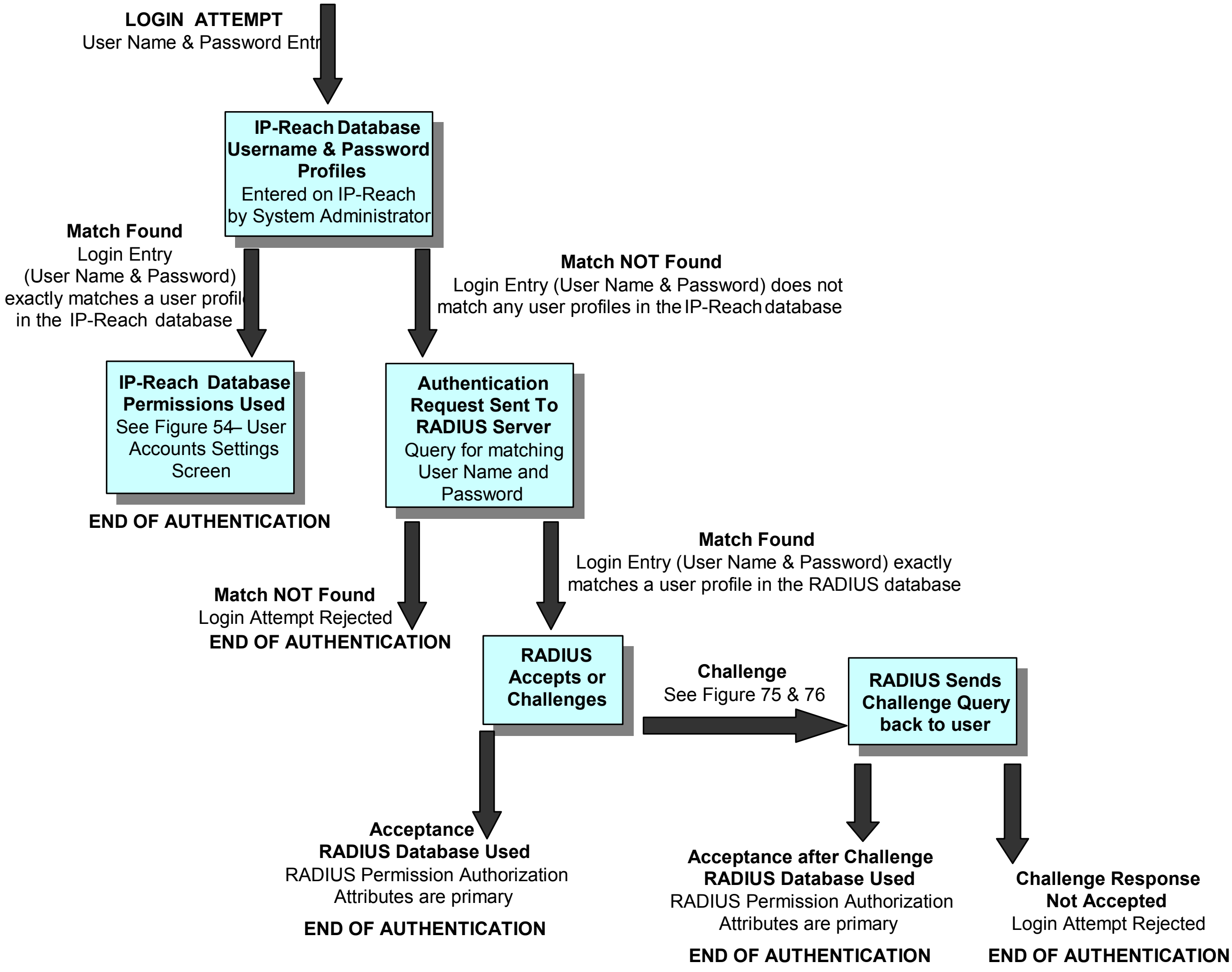
WARNING! Not *all* Sun and Cisco devices have been tested with this cable; you must refer to the user's manual of your device and confirm its pin-out to ensure compatibility. If you are at all unfamiliar with this procedure, you should not attempt to make your own direct-connect cable – instead, use Raritan's standard DB9 and DB25 adapters.

Appendix C: RADIUS Server Settings

This appendix discusses the RADIUS server and how it interacts with Dominion KSX to accommodate Dominion KSX as a RADIUS client. For information on designating the Dominion KSX unit itself as a RADIUS client, see the Radius Configuration section in **Chapter 4: Administrative Menus**.

RADIUS Authentication Priority and Flowchart

When Dominion KSX is configured to utilize RADIUS authentication, user login attempts are first checked against Dominion KSX's internal username and password list. (At least one username/password pair, for the "admin" user, must exist in the Dominion KSX database). Should the login attempt fail and Dominion KSX is configured to utilize an external RADIUS server, Dominion KSX then consults the RADIUS server for completing authentication. This process flow is illustrated below.


LOGIN ATTEMPT
User Name & Password Entr
IP-Reach Database Username & Password Profiles
Entered on IP-Reach by System Administrator
Match Found
Login Entry (User Name & Password) exactly matches a user profil in the IP-Reach database
Match NOT Found
Login Entry (User Name & Password) does not match any user profiles in the IP-Reach database
IP-Reach Database Permissions Used
See Figure 54– User Accounts Settings Screen
END OF AUTHENTICATION
Authentication Request Sent To RADIUS Server
Query for matching User Name and Password
Match NOT Found
Login Attempt Rejected
END OF AUTHENTICATION
Match Found
Login Entry (User Name & Password) exactly matches a user profile in the RADIUS database
RADIUS Accepts or Challenges
Challenge
See Figure 75 & 76
RADIUS Sends Challenge Query back to user
Acceptance
RADIUS Database Used
RADIUS Permission Authorization Attributes are primary
END OF AUTHENTICATION
Acceptance after Challenge
RADIUS Database Used
RADIUS Permission Authorization Attributes are primary
END OF AUTHENTICATION
Challenge Response Not Accepted
Login Attempt Rejected
END OF AUTHENTICATION

Controlling Dominion KSX User Permissions via RADIUS FILTER-ID

Dominion KSX recognizes, and in some cases requires, optional “FILTER-ID” RADIUS attributes that are returned by the RADIUS server. These returned attributes communicate permissions for each user, which override default permissions set for all RADIUS users under the “Default RADIUS Permissions” settings parameter – (see **Chapter 4: Administrative Functions, *RADIUS Configuration***).

The FILTER-ID attribute tells Dominion KSX what permissions to grant or deny each specific RADIUS user (or user group, since most RADIUS servers can be configured to return this optional attribute per user or for groups of users).

The FILTER-ID attribute contains an ASCII text string. The form of the string is the text – “IP-Reach:*letter(s)*” – where *letter(s)* represents one or more of the following case-sensitive parameters that denote access permissions, as follows:

A	Add administrator permissions.
a	Subtract administrator permissions.
K	Add keyboard and mouse control permissions.
k	Subtract keyboard and mouse control permissions.
M	Add modem access permissions.
m	Subtract modem access permissions.
N	Add network access (using Raritan Remote Client software) permissions.
n	Subtract network access (using Raritan Remote Client software) permissions.
V	Add KVM video access permissions
v	Subtract KVM video access permissions
S	Add serial console access permissions.
s	Subtract serial console access permissions.
P	Add PC Share permissions.
p	Subtract PC Share permissions.

Example # 1:

If the “Default RADIUS permissions” option is set to “User permissions (Net,Modem,PC Share)” and the RADIUS server returned a FILTER-ID attribute with the string “IP-Reach:m”, the modem access permission would be removed from the user. The user would be left with Network (Raritan Remote Client Software) and PC Share permissions.

Example # 2:

If the “Default RADIUS permissions” option is set to “None, must use RADIUS attributes” and the RADIUS server returned a FILTER-ID attribute with the string “IP-Reach:NAP”, then the user would have network access, administrator, and PC Share permissions. The user would not have serial console access privileges.

Note: *When the “Default RADIUS permissions” option is set to “None, must use RADIUS attributes,” RADIUS user access to Dominion KSX will be denied unless the FILTER-ID is used to grant the user permissions.*

Note: *To maintain backward compatibility with the existing Raritan installed base, Dominion KSX supports FILTER-ID attributes prefaced by the string "TeleReach:" or “IP-Reach”. Therefore, if you already use Raritan network devices such as TeleReach or IP-Reach, you need not reformat your RADIUS permissions.*

RADIUS Attributes Generated by Dominion KSX

Dominion KSX sends the following RADIUS attributes to the RADIUS server with each access request:

ATTRIBUTE	DATA
USER-NAME	The user name entered at the login screen.
USER-PASSWORD	In PAP mode, the encrypted password entered at the login screen.
CHAP-PASSWORD	In CHAP mode, the CHAP protocol response computed from the password and the CHAP challenge data.
NAS-IP-ADDRESS	Dominion KSX's IP Address
NAS-IDENTIFIER	If the Dominion KSX unit's name, entered at the Dominion KSX Admin Console on the Network Configuration screen, is left to the default name "Dominion KSX," then the identifier will simply be "Dominion KSX". If another name is entered as an alternative to the default name "Dominion KSX," then the identifier will be "Dominion KSX.<name>" where <name> represents the alternative name entered on the Network Configuration screen.
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 a ACCESS-CHALLENGE, the state data from the ACCESS-CHALLENGE packet will be returned.
PROXY-STATE	If this request is in response to a ACCESS-CHALLENGE, the proxy state data from the ACCESS-CHALLENGE packet will be returned.

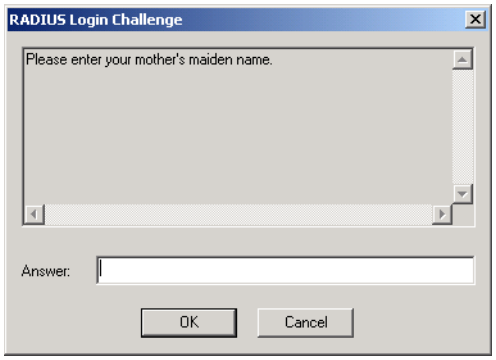
Dominion KSX sends the following RADIUS attributes to the RADIUS server with each accounting request:

ATTRIBUTE	DATA
SESSION-TYPE	Either START (1) for log in or STOP (2) for log out.
SESSION-ID	A string containing a unique session name. The name is in the format of "<NAS-IDENIFIER>:<user IP address>:<number>" where <NAS-IDENTIFER> is the string from the NAS-IDENTIFIER attribute, <user IP address> is the IP address of the user's remote PC, and <number> is a unique sessions number. Example: "Dominion KSX:192.168.1.100:122"
USER-NAME	The user name entered at the login screen.
NAS-IP-ADDRESS	Dominion KSX's IP Address
NAS-IDENTIFIER	If the Dominion KSX unit's name, entered at the Dominion KSX Admin Console on the Network Configuration screen, is left to the default name "Dominion KSX," then the identifier will simply be "Dominion KSX". If another name is entered as an alternative to the default name "Dominion KSX," then the identifier will be "Dominion KSX.<name>" where <name> represents the alternative name entered on the Network Configuration screen.
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 Dominion KSX'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).

RADIUS Access Challenge

A RADIUS server can require additional information from the user in addition to user name and password. The type of information will depend on the authentication method used by the RADIUS server. After Dominion KSX sends the initial ACCESS-REQUEST packet, the RADIUS server can return an ACCESS-CHALLENGE packet. The ACCESS-CHALLENGE packet will contain one or more reply messages for the user. Dominion KSX will display the reply messages and ask for the user's answer to the RADIUS server's challenge.

In the remote application, the RADIUS Challenge dialog box will be displayed after the normal login dialog box. Enter your answer and click on the [**OK**] button.



Please enter your mother's maiden name.

RADIUS challenges will also be asserted at the Dominion KSX Local Admin Console.

Appendix D: SNMP Features

For convenient monitoring with standard network management systems such as HP OpenView or IBM Tivoli software solutions, Dominion KSX features an SNMP agent with standard MIB2 support. Dominion KSX responds to SNMP GET requests with standard MIB2 variables, although for security reasons only a subset of the variables are provided.

Appendix E: Frequently Asked Questions

QUESTION:	ANSWER:
Does Dominion KSX provide an integrated interface that allows you to view both the KVM paths and Serial devices that are connected? What about power control?	Yes, the Dominion KSX graphical user interface (GUI) lets you view and name all of the connected devices – both KVM and serial. In addition, if a Raritan power strip is used, Dominion KSX provides a GUI interface for power control.
Does Dominion KSX provide a local access port?	Dominion KSX includes a local access port for KVM devices. No access port for serial devices is included. However, serial access can be obtained via a Raritan software interface that is always shipped with Dominion KSX.
Can I open multiple windows and "tile" in order to monitor multiple servers and other IT equipment?	Yes, you may monitor and "tile" up to eight serial ports and one KVM connection concurrently per Dominion KSX unit.
Can I use a browser such as Netscape or do I have to use Internet Explorer?	Dominion KSX supports both Netscape and Internet Explorer. However, the browsers must run on a Windows-based server.
What cable does Raritan recommend for use with the KVM ports on Dominion KSX?	Raritan recommends KVM UltraThin cables (CCPT). Raritan's standard cables (CCP) will also work.
Can I use Dominion KSX with my existing Raritan IP-Reach product? Will this combination work to give me an added user?	Yes. The same remote interface is used for both the Dominion KSX and IP-Reach.
Is Dominion KSX easy to install?	Yes. Dominion KSX is very easy to install. It is a true 'plug and play' appliance that does not require an external server to operate.
What level of control does Dominion KSX have over attached Target Servers?	The remote user has direct access and total control of target devices for maintenance, administration and troubleshooting, from running GUI applications to BIOS-level troubleshooting, and even rebooting.
What makes the performance of Dominion KSX different from that of remote access software?	With Dominion KSX, no software runs on each individual target server. Traditional remote access software solutions require software to be loaded and running on each target server, which must offer a supporting operating system. This can create compatibility, performance, and reliability issues on mission critical target servers.
What remote access connection methods can Dominion KSX accommodate?	Dominion KSX provides network administrators with a choice of remote access via Internet, LAN/WAN, or dial-up modem. That means servers can be accessed both in and out of band so remote access to mission critical target servers is always available—even if the network is down.
What is the slowest connection Dominion KSX can handle?	Dominion KSX offers scalable performance based on bandwidth available, down to 20kbps.
Can I use Dominion KSX in a VPN?	Yes, Dominion KSX fits into most any network configuration utilizing TCP/IP. The network administrator simply adds Dominion KSX as a node on the network via Dominion KSX admin console.

Can I perform a Dial-up modem connection to Dominion KSX over a PBX line?	No. Modems require an analog telephone line.
Can I use Dominion KSX within my local network?	Dominion KSX can be used in any computer network that supports TCP/IP.
When does Dominion KSX use TCP? UDP?	Both TCP and UDP are used by Dominion KSX. However, TCP is essential, whereas UDP is optional. UDP is used only for one Dominion KSX feature, automatic detection of Dominion KSX units in a subnet (see **Chapter 3: Raritan Remote Client, *RRC Navigator*)**. If you do not employ the browse feature (and by extension, are not using DHCP), then Dominion KSX will only communicate using TCP.
How are user profile and password information stored on the Dominion KSX unit?	All sensitive data is hashed and stored encrypted for the highest security.

Appendix F: Troubleshooting

Problems and Suggested Solutions

REMOTE CONNECTION PROBLEMS	SOLUTION
I cannot connect to Dominion KSX via dial-up modem.	Ensure that you have specified the modem device for your Remote PC in the Add Connection Window (Dial-up type connection) modem field. Although concurrent connections may be enabled (either globally or individually), the modem in Dominion KSX will only accommodate one remote connection at a time – ensure that someone else is not already connected via modem. Ensure that your user profile has modem access enabled and that Dominion KSX is configured to enable a modem interface on the Network Configuration Screen. Ensure that the communication port chosen by the network administrator on the **Network Configuration** screen matches the port set in your connection profile.
I cannot connect to Dominion KSX via LAN/WAN or Internet.	Re-check the IP settings for Dominion KSX from the Dominion KSX Admin Console or remote **Admin Console** window. Accessing the **Network Configuration** screen, ensure that the IP addresses set for "IP Address, Subnet Mask, and Default Gateway" are still set correctly, per your Network Administrator's instructions. Ensure that your user profile has network access enabled and that Dominion KSX is configured to enable a network interface. Ensure that the communication port chosen by the network administrator on the **Network Configuration** screen matches the port set in your connection profile. Ensure that the network configuration is correct by sending a PING from the Remote PC to Dominion KSX.
I cannot connect to Dominion KSX via Web Browser.	Re-check the IP settings for Dominion KSX from the Dominion KSX Admin Console or remote **Admin Console** window. Accessing the **Network Configuration** screen, ensure that the IP addresses set for "IP Address, Subnet Mask, and Default Gateway" are still set correctly, per your Network Administrator's instructions. Ensure that your user profile has Web Browser access enabled and that Dominion KSX is configured to enable Web Browser.
I cannot connect to Dominion KSX and seem to be stuck at the **Login** window.	Ensure that you are using a valid and correct user name and password. Ensure that you are typing user name and password in the exact upper and lowercase combinations in which they were created. Drag the **Login** window to the side and view **Connection Status** window behind it. The **Connection Status** window will show details on your connection attempts, and may offer specifics on the problem.

TARGET KVM SERVER KEYBOARD PROBLEMS	SOLUTION
Dominion KSX is not accepting keyboard commands from the Remote PC.	The window in Raritan Remote Client that is displaying you Target KVM Server must be the active window for proper keyboard control. Ensure the window in which you are typing is active. Try clearing the keyboard signals to ensure that the release or breakcode signal has been received – alternately press the <**Ctrl**>, <**Shift**> and <**Tab**> keys rapidly a few times on your keyboard. Ensure the remote user has keyboard and mouse privileges. Exit the Dominion KSX software and then restart it again.
I pressed the Caps Lock key on my Remote PC. The CAPS indicator on the Dominion KSX **Status Bar** appeared, but the Caps Lock indicator light is not lit on my Remote PC keyboard.	This is normal. Use the indicators on the **Status Bar** to determine CAPS key status for the Target KVM Server.
The Keyboard is not functioning and the green LED on the back of Dominion KSX for at least one of the KVM ports is not blinking, but rather constantly lit.	Reset the keyboard chips within Dominion KSX by recycling power to it. Make sure you power down both Dominion KSX and all attached KVM switches at the same time. Otherwise the KVM chips in Dominion KSX will draw power from the KVM switches and fail to reset.
I am accessing Dominion KSX via the Web Browser and the keyboard does not function. I type, but nothing happens.	Click the window title bar under the Dominion KSX toolbar to activate the viewing window. If the viewing window is not the active window, the keyboard will not function.

TARGET KVM SERVER MOUSE PROBLEMS	SOLUTIONS
Target KVM Server Mouse Pointer tracks too slowly after Dominion KSX Mouse Pointer. Immediately after switching to a new Target Server channel the mouse stops and/or is out of sync.	When working from a Remote PC, a slight delay between your local mouse pointer and the Target KVM Server's Mouse Pointer is normal due to uncontrollable lags in the speed of the remote connection – Internet, direct dial modem, or network. With each new video image viewed, Dominion KSX automatically re-syncs and aligns the mouse pointers. Wait a few seconds after switching to each new video image for automatic re-calibration to take place and the two mouse pointers will line up with each other. If you do not wish to wait for this auto calibration, or you find the two mouse pointers out of sync at any time; click the **Synchronize Mouse button**, or simultaneously press the keys <**Ctrl-Alt-S**>. This will manually re-align the two pointers. Be sure to follow the directions in **Chapter 2: Installation**, "Configuring Target KVM Servers" in order to ensure that mouse synchronization functions properly.

TARGET KVM SERVER MOUSE PROBLEMS	SOLUTIONS
The local mouse pointer does not track or is not in sync (not aligned) with the Target KVM Server's Mouse Pointer.	Click **Synchronize Mouse button**, or press <Ctrl-Alt-S>. Ensure each Target Server uses a standard Windows mouse driver; the IntelliMouse driver is not currently supported. Be sure to follow the directions in **Chapter 2: Installation**, "Configuring Target KVM Servers" in order to ensure that mouse synchronization functions properly. Click **Auto-sense Video button** or simultaneously press <Ctrl-Alt-A>.
Dominion KSX is not accepting my mouse.	Dominion KSX will not support a serial type mouse or non-standard mouse drivers. It does support a PS/2 style mouse and standard Windows mouse drivers. Other mouse drivers may function with Dominion KSX, but will require extensive changes to the mouse settings until a functioning mix of motion settings is found. If you must use a mouse driver on a Target Server that is not currently supported by Dominion KSX, try setting the mouse acceleration to <none> and the mouse speed to <slow>.
Dominion KSX Mouse Pointer and the **Target Server Mouse Pointer** do not sync up in certain Windows NT Administration screens, like the NT log on screen.	Windows NT Administration or Log On screens may revert to default mouse pointer motion/acceleration speeds. As a result, mouse sync may not be optimal at these screens. If you are comfortable adjusting the registry on the Windows NT Target Server, you can obtain better Dominion KSX mouse sync at NT Administration screens by entering the Target Server's registry editor and changing the following settings: default user mouse motion speed = 0; mouse threshold 1 = 0; mouse threshold 2 = 0.

TARGET KVM SERVER PROBLEMS	SOLUTION
When I reboot a Target KVM Server through Dominion KSX, from a Remote PC, I cannot access the Target Server's BIOS. It seems Dominion KSX is not accepting the BIOS entry command keystroke.	To access a Target Server's BIOS, you may have to first temporarily de-select the **Sense video mode changes automatically** checkbox in the **Video Settings** window, accessed with the **Video Settings** button on the Dominion KSX toolbar. Video auto-sensing slows the remote viewing of the reboot process and makes it difficult to send BIOS access keystrokes to the Target Server from a Remote PC (the BIOS screen prompt passes too quickly). De-selecting the auto-sense checkbox frees Dominion KSX to convey BIOS access keystrokes as quickly as possible. It also aides in the quick interpretation of rapidly changing video screens. Be sure to re-select the checkbox when finished with BIOS access.

TARGET KVM SERVER VIDEO PROBLEMS	SOLUTION
After switching to a different Target Server channel the video is not clear. Sometimes there is a black edge at the boundary of the Target Server's screen.	Click the **Auto-sense Video button** or simultaneously press the keys <**Ctrl-Alt-A**>. Dominion KSX will adjust the video settings. If the video does not become clear, additional manual video setting adjustments may be necessary. Contact Raritan Technical Support to discuss changes to the **Video Settings** window. Ensure all Target Servers have standard blanking times. Horizontal and vertical blanking times should closely approximate VESA standard values.
When viewing a Target Server remotely, the video image is filled with moving block of incorrect color that seem to track next to the movement of the mouse pointer.	The Color Settings on the Video Settings tab in the **Video** window are not set correctly. Attempt manual adjustment until the color blocking ceases or run the Automatic Color Calibration Routine (see **Chapter 3: Raritan Remote Client, *Color Calibration*).**

TARGET KVM SERVER VIDEO PROBLEMS	SOLUTION
The screen is filled with small visual errors, or grains of missing color, which need to be cleaned up.	Click the **Refresh Screen button** on the Dominion KSX toolbar or simultaneously press the keys <**Ctrl-Alt-R**>.
The video seems to be stuck in Auto Sense mode and the auto sensing message in the middle of the screen keeps counting higher and higher.	Pressing the **Auto-sense Video button** while auto sensing is occurring will stop the auto sense process. Check your Target Server resolution to ensure Dominion KSX supports it.

WEB BROWSER PROBLEMS	SOLUTION
Raritan Remote Client does not appear when I attempt to access Dominion KSX via web browser.	Ensure that your Dominion KSX has Web Browser access enabled. Ensure that you are accessing Dominion KSX with a Windows-based computer (Win32), using Internet Explorer, Netscape, or Mozilla. Ensure that your network and firewall configuration allows access to the HTTPS port 443. Ensure that your network and firewall configuration allows access to the HTTP port 80 (if you wish to use the URL "http://" instead of "https://". If you are using Windows NT and higher, and this is the first time you are accessing Dominion KSX via web browser on that computer, ensure that you are not logged in as a "restricted" user. Ensure that your web browser allows ActiveX objects to be downloaded and launched.
When using Raritan Remote Client via web browser, I click on a serial port or the power control port ("PowerPort"), but nothing appears – I only see a blank white screen.	If you are using Windows XP, Microsoft's inconsistent application of Java technology can cause conflicts in your web browser's capability to run Java applets. Be sure that only one Java virtual machine is active on your computer. Many Windows XP users have multiple Java virtual machines from Sun Microsystems – or more likely – both a Microsoft Java virtual machine, as well as a Sun Microsystems Java virtual machine both active. These version conflicts cause Raritan Remote Client's serial console and power control capabilities to cease from executing.

LOCAL ACCESS CONSOLE PROBLEMS	SOLUTION
When using the Local Access Console on the front of Dominion KSX to access Target KVM Servers locally, noise appears on my monitor.	Increase the video resolution of your Target KVM Server. If noise persists, use a CRT monitor instead of an LCD monitor on the Local Access Console port.

Event Log File and On-Screen Error Codes

Dominion KSX will display or log an error code in the **Dominion KSX Event Log Screen** in the event of a problem occurring. Error codes are eight-digit hexadecimal numbers, containing two parts: the first four denote error type; and the second four digits denote a location code.

These last four digits of the Dominion KSX error code are the most useful in determining what has caused a system failure. Below is a list of location codes (the last four digits of an error code), and their meanings.

ERROR CODE (LAST 4 DIGITS)	MEANING	RECOMMENDATION
0001 – 0003	Memory allocation error	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0004	Could not read the onfiguration file on startup. The file may be corrupt, the file system may be damaged, or the config file might be from an older version of Dominion KSX.	Reenter the configuration information and reboot. If the problem continues, restore the software and file system from the Recovery CD-ROM.
0005	The config file was missing. This may be the first time you have started Dominion KSX or the file system has become corrupt.	Reenter the configuration information and reboot. If the problem continues, restore the software and file system from the Recovery CD-ROM.
0006	The config file could not be saved. The file system may be corrupt or the hard drive may not be responding.	Retry, but if the problem persists, restore the software and file system from the Recovery CD-ROM.
0007 – 0008	Memory allocation error.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
Delete	Memory allocation error.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the recovery CD-ROM.
0009	Could not find the frame rabber card.	Power off the system and make sure the frame grabber card is inserted firmly. If the problem persists, there may be a problem with your Dominion KSX hardware.
000A	Frame grabber card is not responding correctly.	Power off the system and make sure the frame grabber card is inserted firmly. If the problem persists, there may be a problem with your Dominion KSX hardware.
000B	Memory allocation error.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
000C – 000F	Memory allocation error.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0011	The Ethernet controller could not be found.	There is a problem with the Dominion KSX hardware.
0012	The modem could not be found.	Power off the system and make sure the frame grabber card is inserted firmly. If the problem persists, there may be a problem with your Dominion KSX hardware.
0013	Memory allocation error.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0014	There is a problem with the IP address.	Check the IP address configuration and reboot.

ERROR CODE (LAST 4 DIGITS)	MEANING	RECOMMENDATION
0015	The DHCP server did not respond. Dominion KSX could not acquire an IP address.	Make sure your DHCP server is operating correctly and then reboot Dominion KSX.
0016 – 0019	There is a problem with one of the Dominion KSX startup files.	Restore the software and file system from the Recovery CD-ROM.
001A	Error occurred while nitializing the UDP socket.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
001B	Error occurred while nitializing the TCP write socket.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
001C	Error occurred while nitializing the TCP read socket.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
001D – 001E	Resource allocation error.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
001F	Could not listen to the TCP write socket.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0020	Could not listen to the TCP read socket.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0021	TCP listen process failed.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0022	UDP listen process failed.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0023	SSL write failed.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0024	SSL read failed.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0025	Memory allocation error.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0026 – 0029	Resource allocation error.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
002A – 002F	Resource allocation error.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0030-0039	Resource allocation error.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.

ERROR CODE (LAST 4 DIGITS)	MEANING	RECOMMENDATION
003A – 003F	Resource allocation error.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0040	Resource allocation error.	Reboot Dominion KSX. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.