Dominion KX II

User Guide

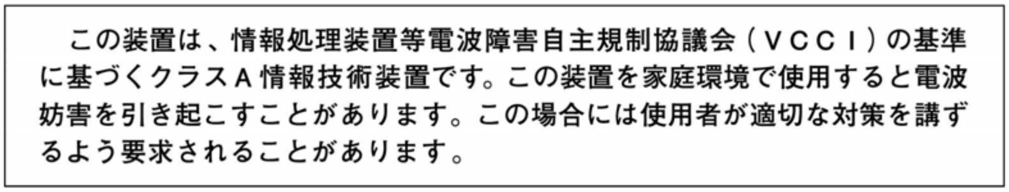
Release 2.0.10

DKX2-0G-E
April 2008
255-62-4023-00

FCC Information

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

VCCI Information (Japan)



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

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

C UL US 1F61
LISTED I.T.E.

Contents

Chapter 1 Introduction 1

Chapter 2 Installation and Configuration 10

Appendix A Specifications 288

Appendix B Updating the LDAP Schema 302

Appendix C Informational Notes 311

Chapter 1 Introduction

In This Chapter

Dominion KX II Overview

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

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

Dominion KX II products can operate as standalone appliances and do not rely on a central management device. For larger data centers and enterprises, numerous Dominion KX II units (along with Dominion SX units for remote serial console access and Dominion KSX for remote/branch office management) can be integrated into a single logical solution using Raritan's CommandCenter Secure Gateway (CC-SG) management unit.

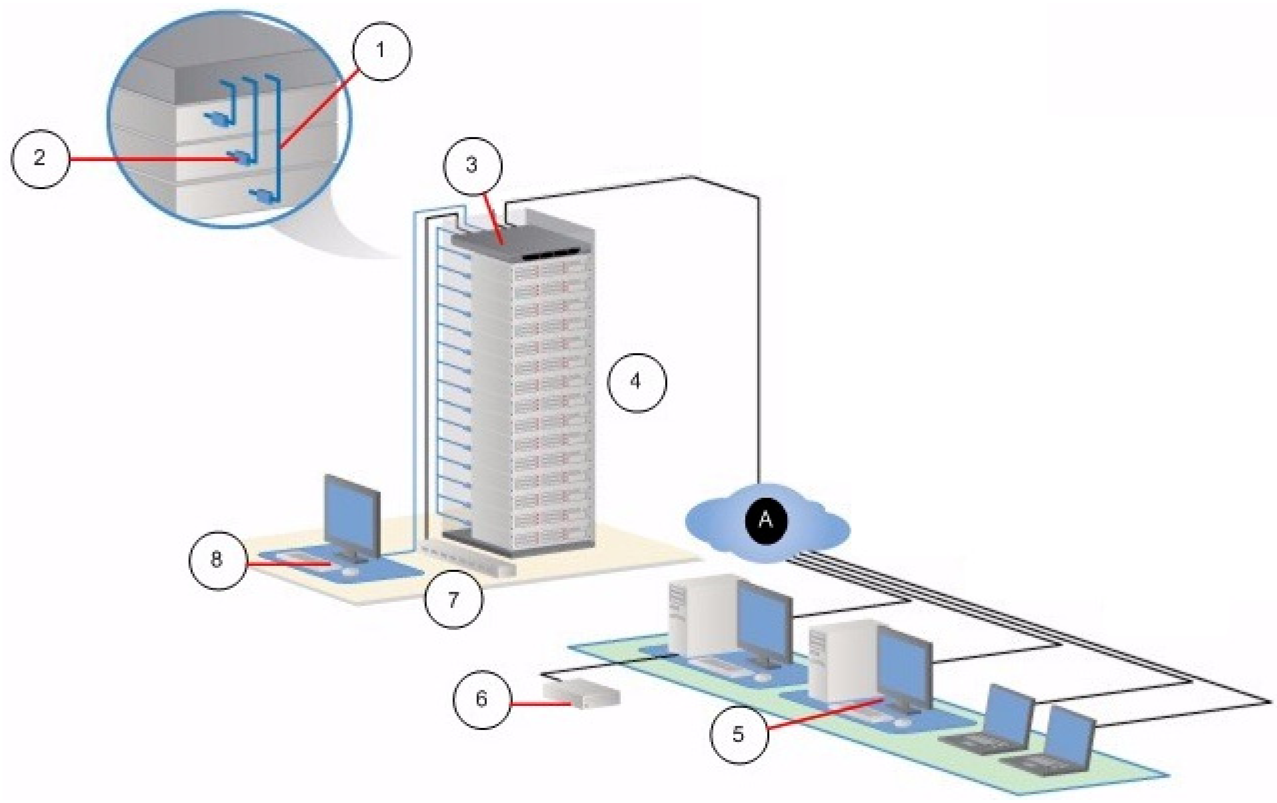


Diagram key			
1	Cat5 cable	6	Remote virtual media USB drive(s)
2	Computer Interface Module (CIM)	7	Power strip
3	Dominion KX II	8	Local access
4	Remote KVM and serial devices	A	IP LAN/WAN
5	Remote (network) access		

Virtual Media

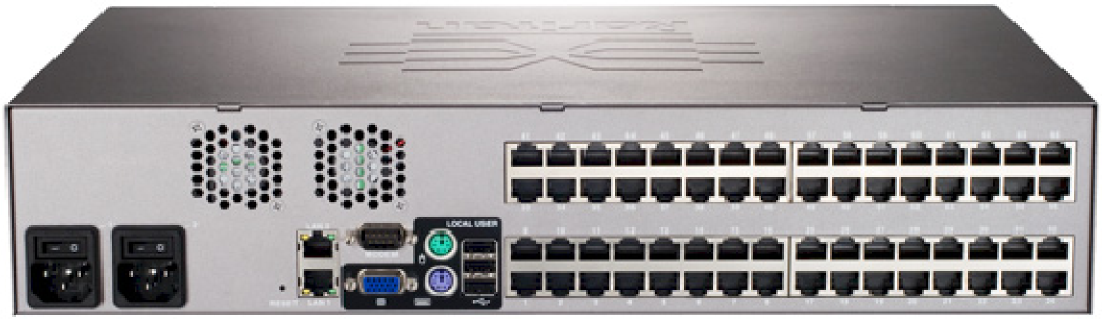
All Dominion KX II models support virtual media. The benefits of virtual media - mounting of remote drives/media on the target server to support software installation, and diagnostics - are now available in all of the Dominion KX II models.

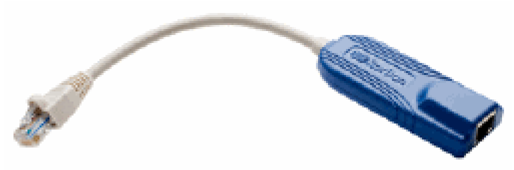
Each Dominion KX II comes equipped with virtual media to enable remote management tasks using the widest variety of CD, DVD, USB, internal and remote drives and images. Unlike other solutions, the Dominion KX II supports virtual media access of hard drives and remotely mounted images for added flexibility and productivity.

Virtual media sessions are secured using 128-bit AES or RC4 encryption.

The D2CIM-VUSB CIM and D2CIM-DVUSB (computer interface module) support virtual media sessions to KVM target servers supporting the USB 2.0 interface. This new CIM also supports Absolute Mouse Synchronization™ as well as remote firmware update.

Product Photos





Product Features

Hardware

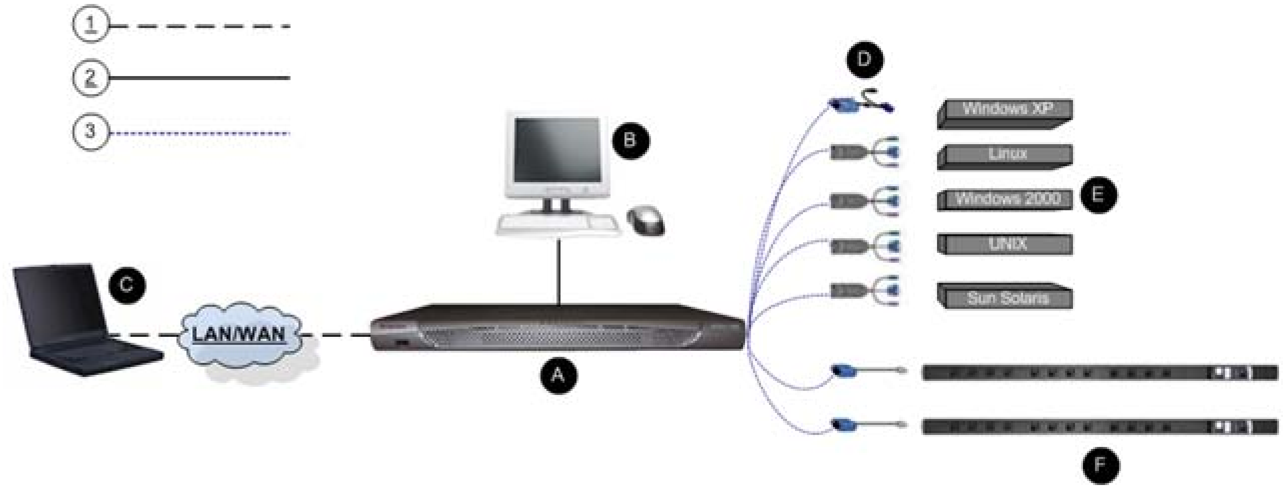
- Integrated KVM-over-IP remote access
- 1U or 2U (KX2-464) rack-mountable; brackets included
- Dual power supplies with failover; autoswitching power supply with power failure warning
- 8, 16, 32, or 64 (on KX2-464) server ports
- Multiple user capacity (1/2/4 remote users; 1 local user)
- UTP (Cat5/5e/6) server cabling
- Dual Ethernet ports (10/100/1000 LAN) with failover
- Field upgradable
- Local user port for in-rack access
  - PS/2 keyboard/mouse ports
  - One front and three back panel USB 2.0 ports for supported USB devices
  - Fully concurrent with remote user access
  - Local graphical user interface (GUI) for administration
- Centralized access security
- Integrated power control
- LED indicators for dual power status, network activity, and remote user status
- Hardware Reset button

Software

- Virtual media with D2CIM-VUSB and D2CIM-DVUSB CIMs
- Absolute Mouse Synchronization with D2CIM-VUSB CIM and D2CIM-DVUSB CIMs
- Plug-and-Play
- Web-based access and management
- Intuitive graphical user interface (GUI)
- 128-bit encryption of complete KVM signal, including video and virtual media
- LDAP, Active Directory, RADIUS, or internal authentication and authorization
- DHCP or fixed IP addressing
- SNMP and Syslog management
- Power control associated directly with servers to prevent mistakes
- Integration with Raritan's CommandCenter Secure Gateway (CC-SG) management unit
- CC Unmanage feature to remove device from CC-SG control

Terminology

This manual uses the following terminology for the components of a typical Dominion KX II configuration:



Terminology

Diagram Key	
①	**TCP/IP**
②	**KVM (Keyboard, Video, Mouse)**
③	**UTP Cable (Cat5/5e/6)**
🅐	**Dominion KX II**
🅑	**Remote PC** Networked computers used to access and control KVM target servers connected to the Dominion KX II. Refer to ***Supported Operating Systems (Clients)*** (on page 290) for a list of the operating systems supported by Dominion KX II remotely.
🅒	**Local Access Console** Local User - an optional user console (consisting of a keyboard, mouse, and multi-sync VGA monitor) attached directly to Dominion KX II to control KVM target servers (directly at the rack, not through the network).
🅓	**CIMS** Dongles that connect to each target server or power strip. Available for all of the supported operating systems. Refer to ***Supported Operating Systems and CIMs (Target Servers)*** (on page 291) for information about the CIMs supported by Dominion KX II.
🅔	**Target Servers** KVM Target Servers - servers with video cards and user interfaces (for example, Windows, Linux, Solaris, etc.) accessed remotely via Dominion KX II. Refer to ***Supported Operating Systems and CIMs (Target Servers)*** (on page 291) for a list of the supported operating systems and CIMs.
🅕	**Dominion PX Power Strips** Raritan power strips accessed remotely via the Dominion KX II.

Package Contents

Each Dominion KX II ships as a fully-configured stand-alone product in a standard 1U (2U for KX2-464) 19" rackmount chassis. Each Dominion KX II unit ships with the following contents:

Amount included	Item
1	Dominion KX II unit
1	Dominion KX II quick installation and setup guide
1	Raritan user guide CD-ROM
1	Rackmount kit
1	AC power cords
1	Cat5 network cable
1	Cat5 network crossover cable
1	Set of 4 rubber feet (for desktop use)
1	Application note
1	Warranty card

User Guide

The Dominion KX II User Guide provides the information to install, set up and configure, access target servers and power strips, use virtual media, manage users and security, and maintain and diagnose the Dominion KX II.

Related Documentation

The Dominion KX II User Guide is also accompanied by a Dominion KX II Quick Setup Guide, which can be found on the CD that accompanied the device or on the Support page of Raritan's website on the Support page (www.raritan.com).

Chapter 2 Installation and Configuration

In This Chapter

This section provides a brief overview of the installation process. Each step is further detailed in the remaining sections of this chapter.

➢ ***To install and configure Dominion KX II:***

- *Step 1: Connect the Equipment* (on page 11)
- *Step 2: Dominion KX II Initial Configuration* (on page 14)
- *Step 3: Configure KVM Target Servers* (on page 21)
- *Step 4 (Optional): Configure Keyboard Language* (on page 34)
- *Step 5: Configure Network Firewall Settings* (on page 35)

Also included in this section is the default logon information you will need. Specifically, the default IP address, user name, and password. See *Default Logon Information* (on page 10).

Getting Started

Default Logon Information

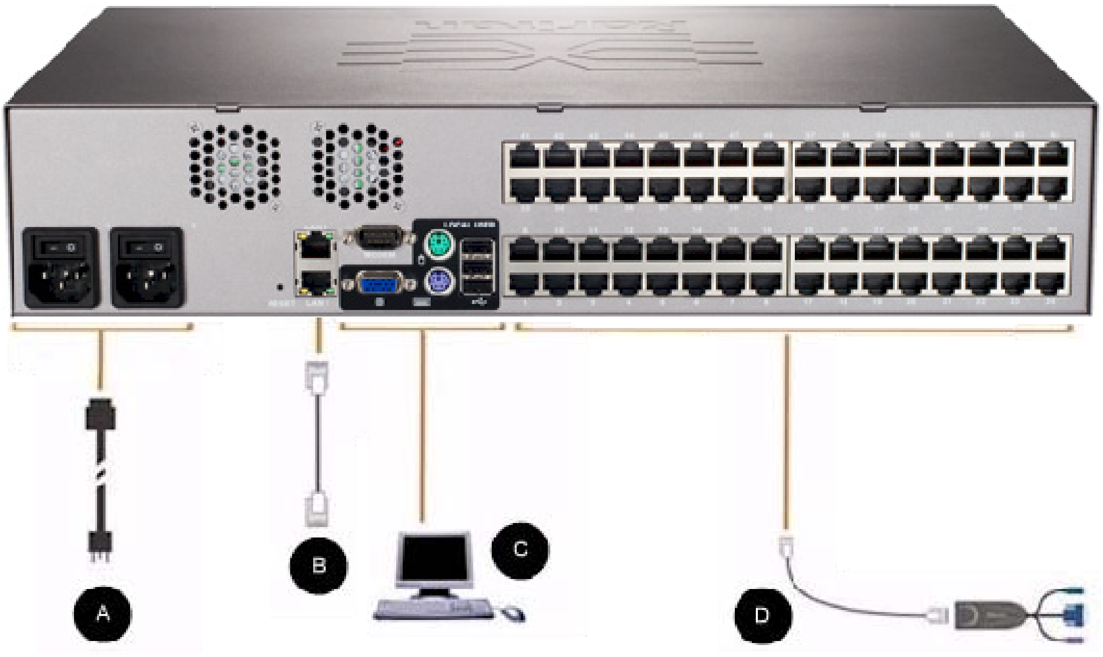
Default	Value
User name	The default user name is admin. This user has administrative privileges.

Default	Value
Password	The default password is raritan. Passwords are case sensitive and must be entered in the exact case combination in which they were created. For example, the default password raritan must be entered entirely in lowercase letters. The first time you start the Dominion KX II, you are required to change the default password.
IP address	Dominion KX II ships with the default IP address of 192.168.0.192.

Tip: For backup and business continuity purposes, it is strongly recommended that you create a backup administrator user name and password and keep that information in a secure location.

Step 1: Connect the Equipment

Connect the Dominion KX II to the power supply, network, local PC, and target servers. The letters in the diagram correspond to the topics in this section that describe the connection.



A. AC Power

➢ *To connect the power supply:*

1. Attach the included AC power cord to the Dominion KX II and plug into an AC power outlet.
2. For dual power failover protection, attach the second included AC power cord and plug it into a different power source than the first power cord.

Note: If you only attach one power cord, the power LED on the Dominion KX II front panel will be red because the system is set to automatically detect both sources. Refer to the ***Power Supply Setup Page*** (on page 233) for information about turning off automatic detection for the power source not in use.

B. Network Ports

Dominion KX II provides two Ethernet ports for failover purposes (not for load-balancing). By default, only LAN1 is active and the automatic failover is disabled. When enabled, if the Dominion KX II internal network interface or the network switch to which it is connected becomes unavailable, LAN2 will be enabled using the same IP address.

Note: Because a failover port is not activated until after a failover has actually occurred, Raritan recommends that you either not monitor the failover port or monitor it only after a failover occurs.

➢ *To connect the network:*

1. Connect a standard Ethernet cable (included) from the network port labeled LAN1 to an Ethernet switch, hub, or router.
2. To make use of the optional Dominion KX II Ethernet failover capabilities:
   - Connect a standard Ethernet cable from the network port labeled LAN2 to an Ethernet switch, hub, or router.
   - Enable Automatic Failover on the Network Configuration page (refer to ***Network Settings*** (on page 219) for more information).

Note: Use both network ports only if you want to use one as a failover port.

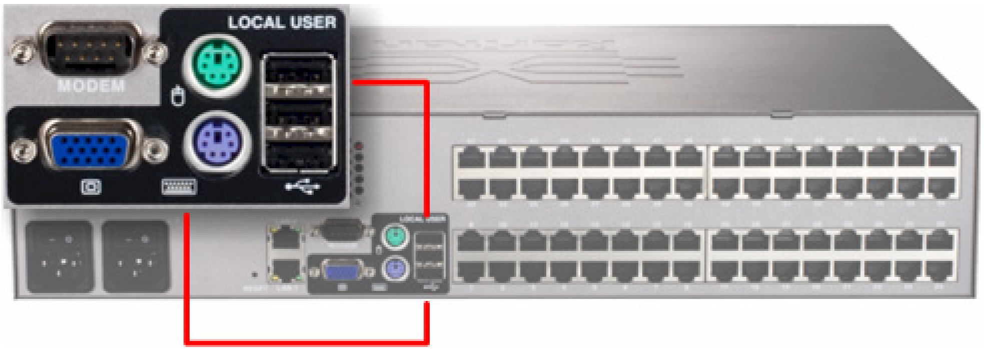
C. Local Access Port (local PC)

For convenient access to target servers while at the rack, use the Dominion KX II Local Access port. While the local port is required for installation and setup, it is optional for subsequent use. The local port provides the Dominion KX II Local Console graphical user interface for administration and target server access.

➢ ***To connect the local port:***

- Attach a multi-sync VGA monitor, mouse, and keyboard to the respective Local User ports (using either a PS/2 or USB keyboard and mouse).

The physical connections for the local ports can be found on the back panel of the Dominion KX II:



Connection	Description
Monitor	Attach a standard multi-sync VGA monitor to the HD15 (female) video port.
Keyboard	Attach either a standard PS/2 keyboard to the Mini-DIN6 (female) keyboard port, or a standard USB keyboard to one of the USB Type A (female) ports.
Mouse	Attach either a standard PS/2 mouse to the Mini-DIN6 (female) mouse port or a standard USB mouse to one of the USB Type A (female) ports.

D. Target Server Ports

The Dominion KX II uses standard UTP cabling (Cat5/5e/6) to connect to each target server. Refer to ***Specifications*** (on page 288) for additional information.

➢ ***To connect a target server to the Dominion KX II:***

1. Use the appropriate Computer Interface Module (CIM). Refer to ***Supported Operating Systems and CIMs (Target Servers)*** (on page 291) for more information about the CIMs to use with each operating system.
2. Attach the HD15 video connector of your CIM to the video port of your target server. Ensure that your target server's video has already been configured to a supported resolution and refresh rate. For Sun servers, also ensure that your target server's video card has been set to output standard VGA (H-and-V sync) and not composite sync.
3. Attach the keyboard/mouse connector of your CIM to the corresponding ports on your target server. Using a standard straight-through UTP (Cat5/5e/6) cable, connect the CIM to an available server port on the back of your Dominion KX II unit.

Note: The DCIM-USB G2 provides a small slide switch on the back of the CIM. Move the switch to P for PC-based USB target servers; move the switch to S for Sun USB target servers.

A new switch position takes effect only after the CIM is power-cycled. To power-cycle the CIM, remove the USB connector from the target server and plug it back in a few seconds later.

Step 2: Dominion KX II Initial Configuration

The first time you power up the Dominion KX II device, there is some initial configuration that you need to perform through the Dominion KX II Local Console:

- Change the default password.
- Assign the IP address.
- Name the KVM target servers.

Changing the Default Password

The Dominion KX II ships with a default password. The first time you start the Dominion KX II you are required to change that password.

➢ ***To change the default password:***

1. Power on the Dominion KX II using the power switch(es) at the back of the unit. Wait for the Dominion KX II unit to boot. (A beep signals that the boot is complete.)
2. Once the unit has booted, the Dominion KX II Local Console is visible on the monitor attached to the Dominion KX II local port. Type the default username (admin) and password (raritan) and click Login. The Change Password screen is displayed.
3. Type your old password (raritan) in the Old Password field.
4. Type a new password in the New Password field and retype the new password in the Confirm New Password field. Passwords can be up to 64 characters in length and can consist of English alphanumeric characters and the special characters.
5. Click Apply.

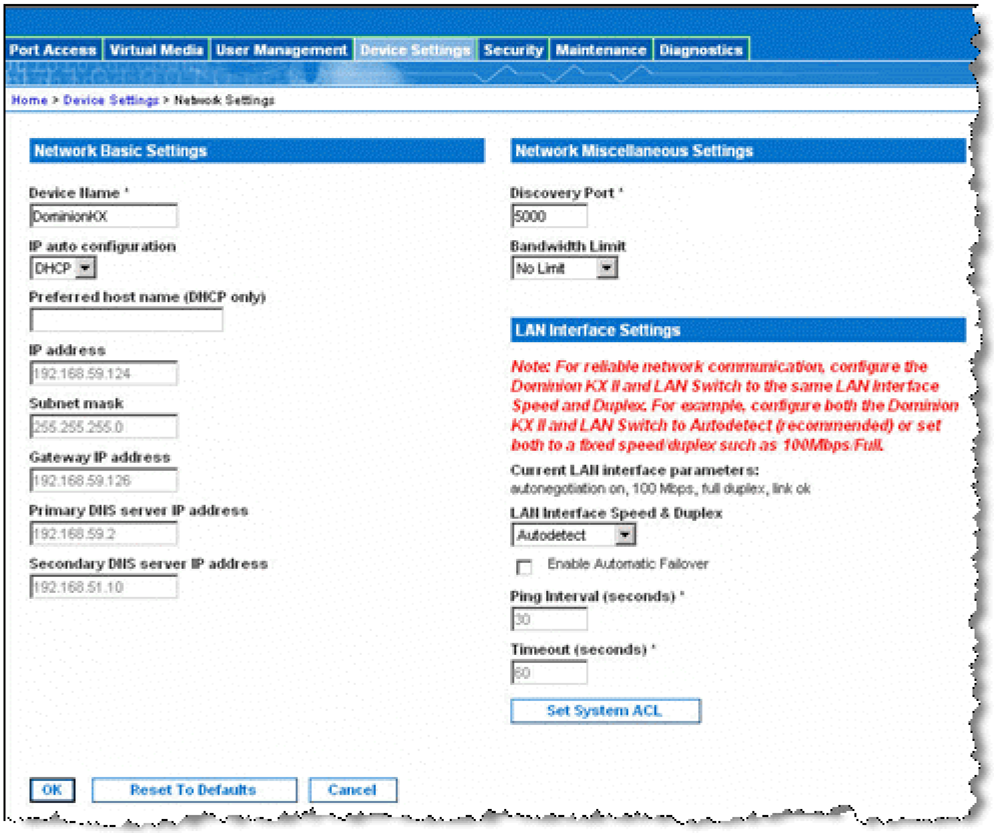
You will receive confirmation that the password was successfully changed. Click OK. The Port Access page is displayed.

Note: The default password can also be changed from the Raritan Multi-Platform Client (MPC).

Assigning an IP Address

These procedures describe how to assign an IP address on the Network Settings page. For complete information about all of the fields and the operation of this page, refer to ***Network Settings*** (on page 219).

1. From the Dominion KX II Local Console, choose Device Settings > Network. The Network Settings page opens.



Network Basic Settings

Device Name *
DominionKX

IP auto configuration
DHCP

Preferred host name (DHCP only)

IP address
192.168.59.124

Subnet mask
255.255.255.0

Gateway IP address
192.168.59.126

Primary DNS server IP address
192.168.59.2

Secondary DNS server IP address
192.168.51.10

Network Miscellaneous Settings

Discovery Port *
5000

Bandwidth Limit
No Limit

LAN Interface Settings

Note: For reliable network communication, configure the Dominion KX II and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX II and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.

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

LAN Interface Speed & Duplex
Autodetect

☐ Enable Automatic Failover

Ping Interval (seconds) *
30

Timeout (seconds) *
60

2. Specify a meaningful Device Name for your Dominion KX II unit using up to 16 alphanumeric characters, special characters, and no spaces.

3. Choose the IP autoconfiguration from the drop-down list:

   - None (Static IP) - This option requires that you manually specify the network parameters. This is the recommended option because the Dominion KX II is an infrastructure device and its IP address should not change.

   - DHCP - With this option, network parameters are assigned by the DHCP server.

4. If you specify an IP configuration of None, type the TCP/IP parameters for your Dominion KX II unit: IP address, Subnet mask, Gateway IP address, Primary DNS server IP address, and optional Secondary DNS server IP address.

5. When finished, click OK. Your Dominion KX II unit is now network accessible.

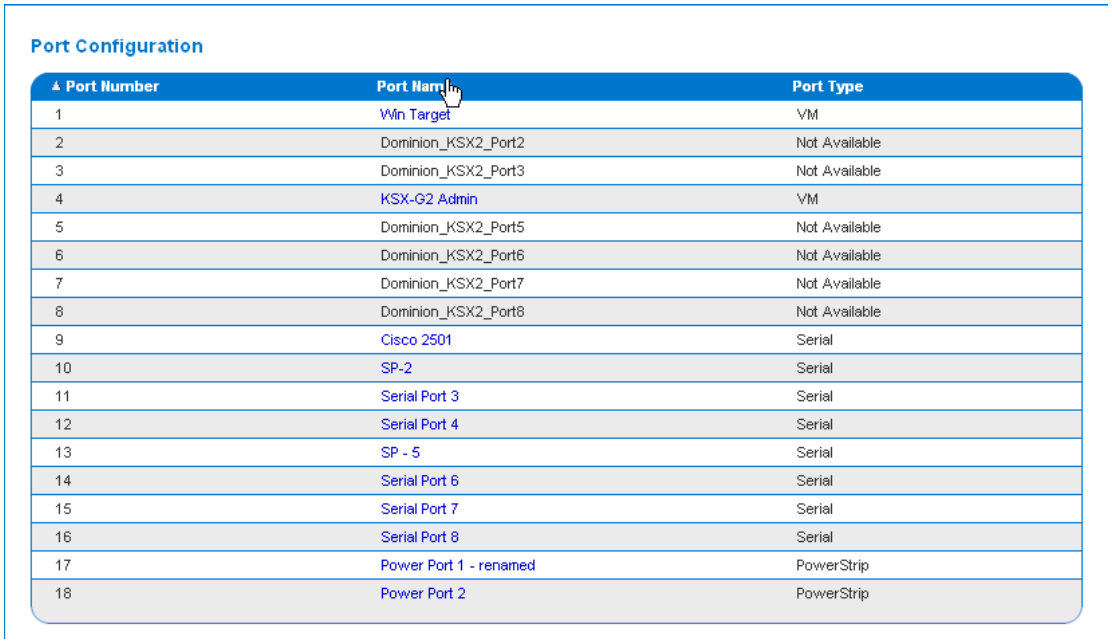
Note: In some environments, the default LAN Interface Speed & Duplex setting Autodetect (autonegotiator) does not properly set the network parameters, which results in network issues. In these instances, setting the Dominion KX II LAN Interface Speed & Duplex field to 100 Mbps/Full Duplex (or whatever option is appropriate to your network) addresses the issue. Refer to the ***Network Settings*** (on page 219) page for more information.

Naming Target Servers

➢ ***To name the target servers:***

1. Connect all of the target servers if you have not already done so (as described in ***Step 1: Connect the Equipment*** (on page 11)).

2. Using the Dominion KX II Local Console, choose Device Settings > Port Configuration. The Port Configuration page opens.



Port Configuration

▲ Port Number	Port Name	Port Type
1	Win Target	VM
2	Dominion_KSX2_Port2	Not Available
3	Dominion_KSX2_Port3	Not Available
4	KSX-G2 Admin	VM
5	Dominion_KSX2_Port5	Not Available
6	Dominion_KSX2_Port6	Not Available
7	Dominion_KSX2_Port7	Not Available
8	Dominion_KSX2_Port8	Not Available
9	Cisco 2501	Serial
10	SP-2	Serial
11	Serial Port 3	Serial
12	Serial Port 4	Serial
13	SP - 5	Serial
14	Serial Port 6	Serial
15	Serial Port 7	Serial
16	Serial Port 8	Serial
17	Power Port 1 - renamed	PowerStrip
18	Power Port 2	PowerStrip

3. Click the Port Name of the target server you want to rename. The Port Page opens.

4. Assign a name to identify the server connected to that port. The name can be up to 32 characters, and alphanumeric and special characters are allowed.

5. Click OK.

Valid Special Characters for Target Names

Character	Description	Character	Description
!	Exclamation point	;	Semi-colon
"	Double quote	=	Equal sign
#	Pound sign	>	Greater than sign
$	Dollar sign	?	Question mark
%	Percent sign	@	At sign
&	Ampersand	[	Left bracket
(	Left parenthesis	\	Backward slash
)	Right parenthesis	]	Right bracket
*	Asterisk	^	Caret
+	Plus sign	_	Underscore
,	Comma	`	Grave accent
-	Dash	{	Left brace
.	Period	|	Pipe sign
/	Forward slash	}	Right brace
<	Less than sign	~	Tilde
:	Colon		

Specifying Power Supply Autodetection

The Dominion KX II provides dual power supplies, and can automatically detect and provide notification regarding the status of these power supplies. Proper configuration ensures that the Dominion KX II sends the appropriate notifications should a power supply fail.

The Power Supply Setup page is configured to automatically detect both power supplies when two power supplies are used. If only one power supply is used in your configuration, you can disable automatic detection from the Power Supply Setup page.

➢ ***To disable power supply autodetection for the power supply not in use:***

1. Using the Dominion KX II Local Console, choose Device Settings > Power Supply Setup. The Power Supply Setup page opens.
2. Clear autodetection for the power supply that you are not using.

For more information, refer to ***Power Supply Setup Page*** (on page 233).

Note to CC-SG Users

If you are using Dominion KX II in a CC-SG configuration, perform the installation steps, and when finished, consult the CommandCenter Secure Gateway User Guide, Administrator Guide, or Deployment Guide to proceed (all found on Raritan's website, www.raritan.com, under Support).

Note: The remainder of this user guide applies primarily to deploying Dominion KX II device(s) without the integration functionality of CC-SG.

Remote Authentication

Note to CC-SG Users

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

For additional information about CC-SG authentication, refer to the CommandCenter Secure Gateway User Guide, Administrator Guide, or Deployment Guide, which can be downloaded from the Support section of the Raritan website (www.raritan.com).

Supported Protocols

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

Note on Microsoft Active Directory

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

Define User Groups and Users

As part of the initial configuration, in order for users to access the Dominion KX II, you will need to define user groups and users.

The Dominion KX II uses system-supplied default user groups and allows you to create groups and specify the appropriate permissions to suit your needs.

User names and passwords are required to gain access to the Dominion KX II. This information is used to authenticate users attempting to access your Dominion KX II.

Refer to ***User Management*** (on page 196) for more information about adding and editing user groups and users.

Step 3: Configure KVM Target Servers

KVM target servers are the computers that will be accessed and controlled via the Dominion KX II. Before installing the Dominion KX II, configure all KVM target servers to ensure optimum performance. This configuration applies only to KVM target servers, not to the client workstations (remote PCs) used to access the Dominion KX II remotely. Refer to ***Terminology*** (on page 7) for additional information.

Desktop Background

For optimal bandwidth efficiency and video performance, KVM target servers running graphical user interfaces such as Windows, Linux, X-Windows, Solaris, and KDE require configuration. The desktop background need not be completely solid; but desktop backgrounds featuring photos or complex gradients might degrade performance.

Mouse Settings

The Dominion KX II operates in several mouse modes:

- ***Absolute Mouse Mode*** (on page 81) (D2CIM-VUSB only)
- ***Intelligent Mouse Mode*** (on page 79) (do not use an animated mouse)
- ***Standard Mouse Mode*** (on page 79)

For both the Standard and Intelligent mouse modes, mouse parameters must be set to specific values, which are described later in this guide.

Mouse parameters do not have to be altered for Absolute Mouse Synchronization but D2CIM-VUSB is required for this mode. Mouse configurations will vary on different target operating systems. Consult your OS documentation for additional detail.

Intelligent mouse mode generally works well on most Windows platforms. Intelligent mouse mode may produce unpredictable results when active desktop is set on the target. For additional information on Intelligent mouse mode, refer to ***Intelligent Mouse Synchronization Conditions*** (on page 149).

Operating System Mouse and Video Settings

This section provides video mode and mouse information specific to the operating system in use on the target server.

Windows XP/Windows 2003 Settings

➢ ***To configure KVM target servers running Microsoft Windows XP/2003:***

1. Configure the mouse settings:
    a. Choose Start > Control Panel > Mouse.
    b. Click the Pointer Options tab.
    c. In the Motion group:

- Set the mouse motion speed setting to exactly the middle speed.
- Disable the Enhanced pointer precision option.
- Disable the Snap To option.
- Click OK.

Note: When you are running Windows 2003 on your target server, if you access the server via KVM and perform any one off the actions listed below, mouse synchronization may be lost if it has been previously enabled. You will need to select the Synchronize Mouse command from the Mouse menu in the client to enable it again. Following are the actions that may cause this to occur:

- Opening a text editor.

- Accessing the Mouse Properties, Keyboard Properties, and Phone and Mode Options from the Windows Control Panel.

2. Disable transition effects:

   a. Select the Display option from the Control Panel.

   b. Click the Appearance tab.

   c. Click the Effects button.

   d. Deselect the "Use the following transition effect for menus and tooltips" option.

   e. Click OK.

   f. Close the Control Panel.

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

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

WARNING! Proceed only if you are comfortable adjusting the registry on Windows KVM target servers. You can obtain better Dominion KX II mouse synchronization at login pages by using the Windows registry editor to change the following settings (HKEY_CURRENT_USER\Control Panel\Mouse): MouseSpeed = 0; MouseThreshold 1= 0; MouseThreshold 2 = 0.

Windows 2000 Settings

➢ ***To configure KVM target servers running Microsoft Windows 2000:***

1. Configure the mouse settings:
   a. Choose Start > Control Panel > Mouse.
   b. Click the Motion tab.
      - Set the acceleration to None.
      - Set the mouse motion speed setting to exactly the middle speed.
      - Click OK.
2. Disable transition effects:
   a. Select the Display option from the Control Panel.
   b. Click the Effects tab.
   c. Deselect the "Use the following transition effect for menus and tooltips" option.
   d. Click OK.
   e. Close the Control Panel.

Linux Settings (Red Hat 9)

Note: The following settings are optimized for Standard Mouse mode only.

➢ ***To configure KVM target servers running Linux (graphical user interface):***

1. Configure the mouse settings:
   a. Choose Main Menu > Preferences > Mouse. The Mouse Preferences dialog appears.
   b. Click the Motion tab.
   c. Within the Speed group, set the Acceleration slider to the exact center.
   d. Within the Speed group, set the Sensitivity towards low.
   e. Within the Drag & Drop group, set the Threshold towards small.
   f. Close the Mouse Preferences dialog.

   Note: If these steps do not work, issue the xset mouse 1 1 command as described in the Linux command line instructions.

2. Configure the screen resolution:
   a. Choose Main Menu > System Settings > Display. The Display Settings dialog appears.
   b. From the Display tab, select a Resolution supported by Dominion KX II.
   c. From the Advanced tab, verify that the Refresh Rate is supported by Dominion KX II.

Note: Once connected to the target server, in many Linux graphical environments, the <Ctrl> <Alt> <+> command will change the video resolution, scrolling through all available resolutions that remain enabled in the XF86Config file.

➢ ***To configure KVM target servers running Linux (command line):***

1. Set the mouse acceleration to exactly 1 and set the threshold to exactly 1. Enter this command: *xset mouse 1 1*. This should be set for execution upon login.

2. Ensure that each target server running Linux is using a resolution supported by Dominion KX II at a standard VESA resolution and refresh rate.
3. Each Linux target server should also be set so the blanking times are within +/- 40% of VESA standard values:
    a. Go to the Xfree86 Configuration file XF86Config.
    b. Using a text editor, disable all non-Dominion KX II supported resolutions.
    c. Disable the virtual desktop feature (not supported by Dominion KX II).
    d. Check blanking times (+/- 40% of VESA standard).
    e. Restart computer.

Note: If you change the video resolution, you must log off of the target server and log back in for the video settings to take effect.

Note for Red Hat 9 KVM Target Servers

If you are running Red Hat 9 on the target server using a USB CIM, and are experiencing problems with the keyboard and/or mouse, there is an additional configuration setting you can try.

Tip: You might have to perform these steps even after a fresh OS installation.

➢ ***To configure Red Hat 9 servers using USB CIMs:***

1. Locate the configuration file (usually /etc/modules.conf) in your system.
2. Using the editor of your choice, make sure that the alias usb-controller line in the modules.conf file is as follows:

    ```
    alias usb-controller usb-uhci
    ```

    Note: If there is another line using usb-uhci in the /etc/modules.conf file, it needs to be removed or commented out.
3. Save the file.
4. Reboot the system in order for the changes to take effect.

Linux Settings (Red Hat 4)

Note: The following settings are optimized for Standard Mouse mode only.

➢ *To configure KVM target servers running Linux (graphical user interface):*

1. Configure the mouse settings:
   a. Choose Main Menu > Preferences > Mouse. The Mouse Preferences dialog appears.
   b. Open the Motion tab.
   c. Within the Speed group, set the Acceleration slider to the exact center.
   d. Within the Speed group, set the Sensitivity towards low.
   e. Within the Drag & Drop group, set the Threshold towards small.
   f. Close the Mouse Preferences dialog.

   Note: If these steps do not work, issue the xset mouse 1 1 command as described in the Linux command line instructions.

2. Configure the screen resolution:
   a. Choose Main Menu > System Settings > Display. The Display Settings dialog appears.
   b. On the Settings tab, select a Resolution supported by the Dominion KX II.
   c. Click OK.

Note: If you change the video resolution, you must log off of the target server and log back in for the video settings to take effect.

Windows Vista

➢ *To configure KVM target servers running Microsoft Windows Vista:*

1. Configure the mouse settings:
   a. Choose Start > Settings > Control Panel > Mouse.
   b. Click the Pointer Options tab.
   c. In the Motion group:

    - Set the mouse motion speed setting to exactly the middle speed.
    - Disable the "Enhanced pointer precision" option.
    - Click OK.

2. Disable animation and fade effects:
    a. Select the System option from the Control Panel.
    b. Select "Advanced system settings". The System Properties dialog appears.
    c. Click the Advanced tab.
    d. Click the Settings button in the Performance group. The Performance Options dialog appears.
    e. Under Custom options, deselect the following checkboxes:
    - Animation options:
        - Animate controls and elements inside windows
        - Animate windows when minimizing and maximizing
    - Fade options:
        - Fade or slide menus into view
        - Fade or slide ToolTips into view
        - Fade out menu items after clicking
3. Click OK.
4. Close the Control Panel.

SUSE Linux 10.1 Settings

Note: Do not attempt to synchronize the mouse at the SUSE login prompt. You must be connected to the target server to synchronize the mouse cursors.

➢ ***To configure the mouse settings:***

1. Choose Desktop > Control Center. The Desktop Preferences dialog appears.
2. Click Mouse. The Mouse Preferences dialog appears.
3. Open the Motion tab.
4. Within the Speed group, set the Acceleration slider to the exact center position.

5. Within the Speed group, set the Sensitivity slider to low.
6. Within the Drag & Drop group, set the Threshold slider to small.
7. Click Close.

➢ ***To configure the video:***

1. Choose Desktop Preferences > Graphics Card and Monitor. The Card and Monitor Properties dialog appears.
2. Verify that a Resolution and Refresh Rate is in use that is supported by Dominion KX II. Refer to ***Supported Video Resolutions*** (on page 288) for more information.

   Note: If you change the video resolution, you must log off of the target server and log back in for the video settings to take effect.

Make Linux Settings Permanent

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

➢ ***To make your settings permanent in Linux (prompt):***

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

Tip: If you do not want to be prompted upon log off, follow these procedures instead.

➢ ***To make your settings permanent in Linux (no prompt):***

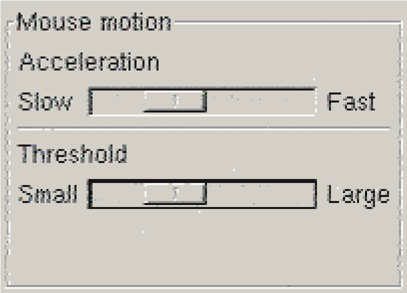
1. Choose Main Menu > Preferences > More Preferences > Sessions. The Session dialog appears.
2. Click the Session Options tab.
3. Deselect the "Prompt on the log off" checkbox.

4. Select the "Automatically save changes to the session" checkbox and click OK. This option automatically saves your current session when you log off.

Sun Solaris Settings

➢ ***To configure KVM target servers running Sun Solaris:***

1. Set the mouse acceleration value to exactly 1 and the threshold to exactly 1. This can be performed from:
   - The graphical user interface:



   - The command line: `xset mouse a t` (where "a" is the acceleration and "t" is the threshold.)

2. All KVM target servers must be configured to one of the display resolutions supported by Dominion KX II. The most popular supported resolutions for Sun machines are:

Display resolution	Vertical refresh rate	Aspect ratio
1600 x 1200	75 Hz	4:3
1280 x 1024	60,75,85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60,70,75,85 Hz	4:3
800 x 600	56,60,72,75,85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60,72,75,85 Hz	4:3

3. KVM 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 nondefault VGA output:***

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

You can also contact your Raritan representative to purchase a video output adapter:

If you have:	Use this video output adapter:
Sun 13W3 with composite sync output	APSSUN II Guardian converter
Sun HD15 with composite sync output	1396C converter to convert from HD15 to 13W3 and an APSSUN II Guardian converter to support composite sync
Sun HD15 with separate sync output	APKMSUN Guardian converter

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

Mouse Settings

- ***To configure the mouse settings (Sun Solaris 10.1):***

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

Accessing the Command Line

1. Right click.
2. Choose Tools > Terminal. A terminal window opens. (It is best to be at the root to issue commands.)

Video Settings (POST)

Sun systems have two different resolution settings: a POST resolution and a GUI resolution. Run these commands from the command line.

Note: 1024x768x75 is used as an example here; substitute the resolution and refresh rate you are using.

➢ ***To check current POST resolution:***

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

➢ ***To change POST resolution:***

1. Run `# eeprom output-device=screen:r1024x768x75`.
2. Log off or restart computer.

Video Settings (GUI)

The GUI resolution can be checked and set using different commands depending on the video card in use. Run these commands from the command line.

Note: 1024x768x75 is used as an example here; substitute the resolution and refresh rate you are using.

Card	To check resolution:	To change resolution:
32-bit	# /usr/sbin/pgxconfig -prconf	1. # /usr/sbin/pgxconfig -res 1024x768x75 2. Log off or restart computer.
64-bit	# /usr/sbin/m64config -prconf	1. # /usr/sbin/m64config -res 1024x768x75 2. Log off or restart computer.
32-bit and 64-bit	# /usr/sbin/fbconfig -prconf	1. # /usr/sbin/fbconfig -res 1024x768x75 2. Log off or restart computer.

IBM AIX 5.3 Settings

Follow these steps to configure KVM target servers running IBM AIX 5.3.

➢ *To configure the mouse:*

1. Go to Launcher.
2. Choose Style Manager.
3. Click Mouse. The Style Manager - Mouse dialog appears.
4. Use the sliders to set the Mouse acceleration to 1.0 and Threshold to 1.0.
5. Click OK.

➢ *To configure the video:*

1. From the Launcher, select Application Manager.
2. Select System_Admin.
3. Choose Smit > Devices > Graphic Displays > Select the Display Resolution and Refresh Rate.
4. Select the video card in use.
5. Click List. A list of display modes is presented.
6. Select a resolution and refresh rate supported by the Dominion KX II. Refer to ***Supported Video Resolutions*** (on page 288) for more information.

Note: If you change the video resolution, you must log off of the target server and log back in for the video settings to take effect.

Make UNIX Settings Permanent

Note: These steps may vary slightly depending on the type of UNIX® (for example, Solaris, IBM AIX) and the specific version in use.

1. Choose Style Manager > Startup. The Style Manager - Startup dialog appears.
2. On the Logout Confirmation dialog, select the On option. This option prompts you to save your current session when you log off.

Apple Macintosh Settings

For KVM target servers running an Apple Macintosh operating system, the preferred method is to use the D2CIM-VUSB and Absolute Mouse Synchronization.

Note: Enable the "Absolute Mouse Scaling for the Mac server" option on the Dominion KX II Port page.

Step 4 (Optional): Configure Keyboard Language

Note: This step is not required if you are using the US/International language keyboard.

If you are using a non-US language, the keyboard has to be configured for the appropriate language. In addition, the keyboard language for the client machine and the KVM target servers has to match.

Consult the documentation for your operating system for additional information about changing the keyboard layout.

Change the Keyboard Layout Code (Sun Targets)

Use this procedure if you are using a DCIM-SUSB and would like the keyboard layout changed to another language.

➢ ***To change the keyboard layout code (DCIM-SUSB only):***

1. Open a Text Editor window on the Sun workstation.
2. Check that the Num Lock key is active and press the left Ctrl key and the Del key on your keyboard. The Caps Lock light starts to blink, indicating that the CIM is in Layout Code Change mode. The text window displays: `Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX)`.
3. Type the layout code desired (for example, *31* for the Japanese keyboard).
4. Press Enter.
5. Shut down the device and power on once again. The DCIM-SUSB performs a reset (power cycle).
6. Verify that the characters are correct.

Step 5: Configure Network Firewall Settings

To access Dominion KX II through a network firewall via Multi-Platform Client or through the Port Access page, your firewall must allow communication on TCP Port 5000 or another port that you designate. Refer to ***Network Settings*** (on page 219) for additional information about designating another discovery port.

To take advantage of the Dominion KX II:	**The firewall must allow inbound communication on:**
Web-access capabilities	Port 443 - standard TCP port for HTTPS communication
Automatic redirection of HTTP requests to HTTPS (so the more common "http://xxx.xxx.xxx.xxx" can be used instead of "https://xxx.xxx.xxx.xxx")	Port 80 - standard TCP port for HTTP communication

Chapter 3 Working with Target Servers

In This Chapter

Interfaces

There are several user interfaces in the Dominion KX II providing you with easy access any time, anywhere. These include the Dominion KX II Local Console, the Dominion KX II Remote Console, and the Multi-Platform Client (MPC). The following table identifies these interfaces and their use for target server access and administration locally and remotely:

	Local		Remote	
User Interface	Access	Admin	Access	Admin
Dominion KX II Local Console	✓	✓		
Dominion KX II Remote Console			✓	✓
Virtual KVM Client			✓	
Multi-Platform Client (MPC)			✓	✓

The following sections of the user guide contain information about using specific interfaces to access the Dominion KX II and manage targets:

- Local Console
- Remote Console
- Virtual KVM Client
- Multi-Platform Client

Dominion KX II Local Console: Dominion KX II Devices

When you are located at the server rack, Dominion KX II provides standard KVM management and administration via the Dominion KX II Local Console. The Dominion KX II Local Console provides a direct KVM (analog) connection to your connected servers; the performance is exactly as if you were directly connected to the server's keyboard, mouse, and video ports.

There are many similarities among the Dominion KX II Local Console and the Dominion KX II Remote Console graphical user interfaces. Where there are differences, they are noted in the user guide. The following options are available in the Dominion KX II Local Console but not the Dominion KX II Remote Console:

- Dominion KX II Local Console Local Port Settings
- Dominion KX II Local Console Factory Reset

Dominion KX II Remote Console Interface

The Dominion KX II Remote Console is a browser-based graphical user interface that allows you to access KVM target servers and serial targets connected to the Dominion KX II and to remotely administer the Dominion KX II.

The Dominion KX II Remote Console provides a digital connection to your connected KVM target servers. When you access a KVM target server using the Dominion KX II Remote Console, a Virtual KVM Client window is opened.

There are many similarities among the Dominion KX II Local Console and the Dominion KX II Remote Console graphical user interfaces, and where there are differences, they are noted in the user manual. The following options are available in the Dominion KX II Remote Console but not the Dominion KX II Local Console:

- Virtual Media
- Favorites
- Backup/Restore
- Firmware Upgrade
- Upgrade Report
- Diagnostics
- USB Profile Selection
- USB Profile Management

Launching the Dominion KX II Remote Console

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

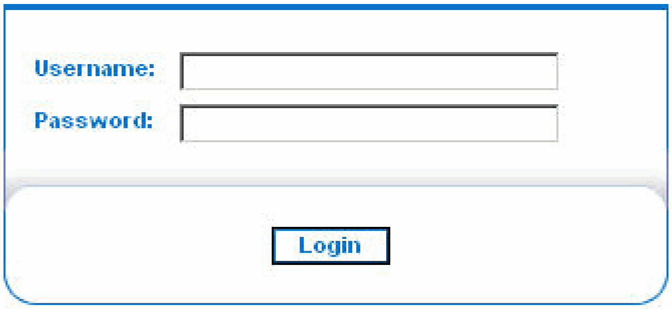
Depending on your browser and security settings, you may see various security and certificate warnings. It is necessary to accept these warnings to launch the Dominion KX II Remote Console.

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

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

➢ *To launch the Dominion KX II Remote Console:*

1. Log on to any workstation with network connectivity to your Dominion KX II and Java Runtime Environment v1.4.2_05 or higher installed (JRE is available at ***http://java.sun.com/*** http://java.sun.com).
2. Launch a supported web browser such as Internet Explorer (IE) or Firefox.
3. Type the following URL: *http://IP-ADDRESS*, where IP-ADDRESS is the IP address that you assigned to your Dominion KX II. You can also use https, the DNS name of the Dominion KX II assigned by the administrator (provided that a DNS server has been configured), or just simply type the IP address in the browser (Dominion KX II always redirects the IP address from HTTP to HTTPS.) The Logon page opens.



4. Type your user name and password. If this is the first time logging on, log on with the factory default user name (admin) and password (raritan, all lower case). You will be prompted to change the default password. Refer to ***Changing the Default Password*** (on page 15) for more information.
5. Click Login.

6. See *Virtual KVM Client* (on page 50) for information on the Dominion KX II functions available via the Remote Console.

Dominion KX II Console Layout

Both the Dominion KX II Remote Console and the Dominion KX II Local Console interfaces provide an HTML (web-based) interface for configuration and administration, as well as target server list and selection. The options are organized into various tabs.

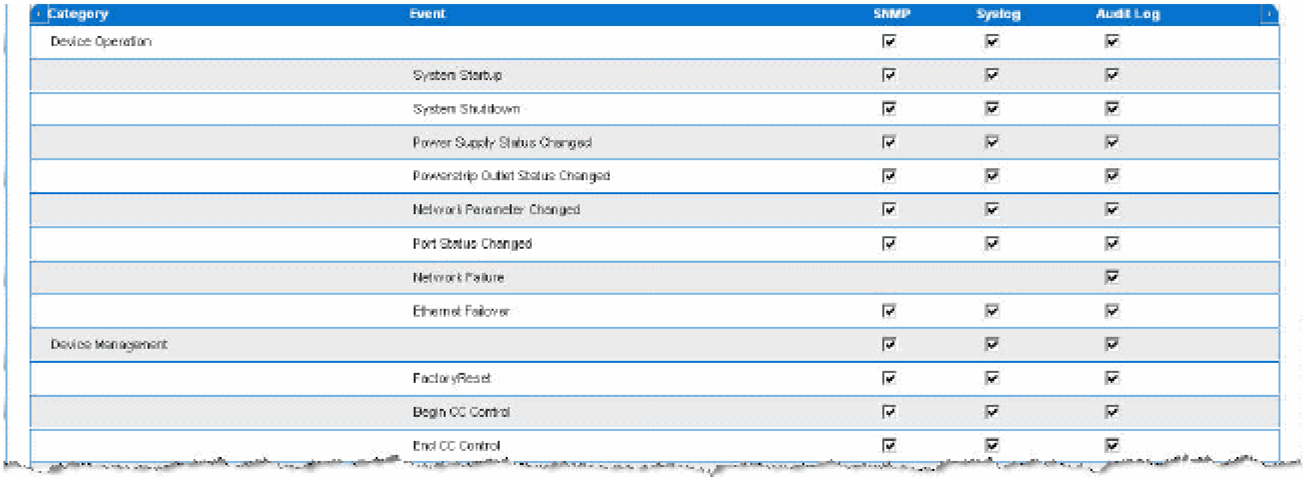
After successful login, the Port Access page opens listing all ports along with their status and availability. You can sort by Port Number, Port Name, Status (Up and Down), and Availability (Idle, Connected, Busy, Unavailable, and Connecting) by clicking on the column heading.

Dominion KX II Console Navigation

The Dominion KX II Console interfaces (both local and remote) provide many methods for navigation and making your selections.

➢ ***To select an option (use any of the following):***

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



Category	Event	SNMP	Syslog	Audit Log
Device Operation		☑	☑	☑
	System Startup	☑	☑	☑
	System Shutdown	☑	☑	☑
	Power Supply Status Changed	☑	☑	☑
	Powerstrip Outlet Status Changed	☑	☑	☑
	Network Parameter Changed	☑	☑	☑
	Port Status Changed	☑	☑	☑
	Network Failure			☑
	Ethernet Failover	☑	☑	☑
Device Management		☑	☑	☑
	FactoryReset	☑	☑	☑
	Begin CC Control	☑	☑	☑
	End CC Control	☑	☑	☑

➢ ***To scroll through pages longer than the screen:***

- Use Page Up and Page Down keys on your keyboard, or
- Use the scroll bar on the right
-

Port Access Page

After successfully logging on to the Dominion KX II Remote Console, the Port Access page opens. This page lists all of the Dominion KX II ports, the connected KVM target servers, and their status and availability. The Port Access page provides access to the KVM target servers connected to the Dominion KX II. KVM target servers are servers that you want to control through the Dominion KX II unit; they are connected to the Dominion KX II ports at the back of the unit.

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

➢ ***To use the Port Access page:***

1. From the Dominion KX II Remote Console, click the Port Access tab. The Port Access page opens.

   The KVM target servers are initially sorted by Port Number; you can change the display to sort on any of the columns.

   - Port Number. Numbered from 1 to the total number of ports available for the Dominion KX II unit. Note that ports connected to power strips will not be among those listed, resulting in gaps in the Port Number sequence.
   - Port Name. The name of the Dominion KX II port; initially set to Dominion-KX2-Port#, but you can change the name to something more descriptive. When you click a Port Name link, the Port Action Menu is opened.
   - Status. The status is either up or down.
   - Availability. The Availability can be Idle, Connected, Busy, or Unavailable.

2. Click the Port Name of the target server you want to access. The Port Action Menu is displayed. Refer to ***Port Action Menu*** (on page 42) for more information about the menu options available.
3. Choose the desired menu command from the Port Action Menu.

➢ ***To change the display sort order:***

- Click the column heading you want to sort on. The list of KVM target servers is sorted by that column.

Port Action Menu

When you click a Port Name in the Port Access list, the Port Action menu is displayed. Choose the desired menu option for that port to execute it. Note that only options available for the selected port are listed in the Port Action menu:

- Connect. Creates a new connection to the target server. For the Dominion KX II Remote Console, a new ***Virtual KVM Client*** (on page 50) window is opened. For the Dominion KX II Local Console, the display switches to the target server and switches away from the local user interface. On the local port, the Dominion KX II Local Console interface must be visible in order to perform the switch.

Note: This option is not available from the Dominion KX II Remote Console for an available port if all connections are busy.

- Switch From. Switches from an existing connection to the selected port (KVM target server). This menu item is available only for KVM targets. This option is visible only when a Virtual KVM Client is opened.

Note: This menu item is not available on the Dominion KX II Local Console.

- Disconnect. Disconnects this port and closes the Virtual KVM Client window for this target server. This menu item is available only when the port status is up and connected, or up and busy.

Note: This menu item is not available on the Dominion KX II Local Console; the only way to disconnect from the switched target in the Local Console is to use the ***hot key*** (see "Hotkeys" on page 282).

- Power On. Powers on the target server through the associated outlet. This option is visible only when there is one or more power associations to the target.
- Power Off. Powers off the target server through the associated outlets. This option is visible only when there is one or more power associations to the target, when the target power is on (port status is up), and when user has permission to operate this service.

- Power Cycle. Power cycles the target server through the associated outlets. This option is visible only when there is a power association (one or more) to this target and when the user has permission to operate this service.

Managing Favorites

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

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

Note: This feature is available only on the Dominion KX II Remote Console (not the Dominion KX II Local Console).

➢ *To access a favorite Dominion KX II device:*

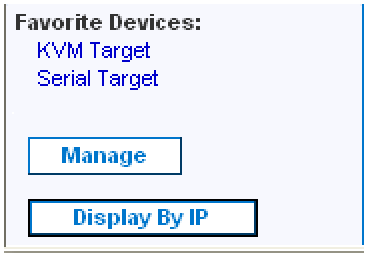
- Click the device name (listed beneath Favorite Devices). A new browser opens to that device.

➢ *To toggle the favorite devices list display between name and IP Address:*

To display Favorites by IP Address:

- Click the Display by IP button.

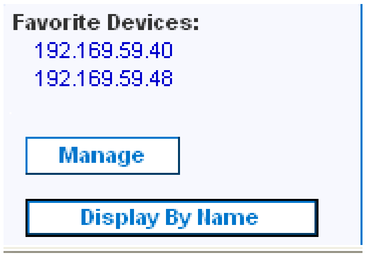
Favorite Devices currently displayed by name; Click Display by IP to toggle.



To display Favorites by name:

- Click the Display by Name button.

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

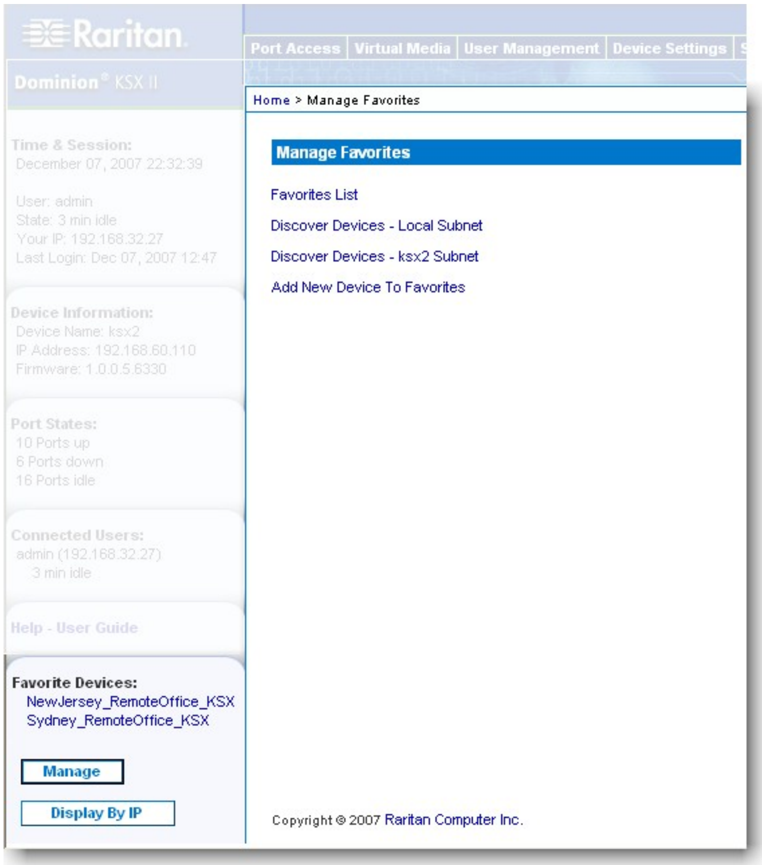


Manage Favorites Menu

➢ To open the Manage Favorites page:

- Click the Manage button in the left panel. The Manage Favorites page opens and contains the following:

Use:	To:
Favorites List	Manage your list of favorite devices.
Discover Devices - Local Subnet	Discover the devices on the local subnet.
Discover Devices - Dominion KX II Subnet	Discover the devices on the Dominion KX II device subnet.
Add New Device to Favorites	Add, edit, and delete devices from your list of Favorites.



Time & Session:
December 07, 2007 22:32:39

User: admin
State: 3 min idle
Your IP: 192.168.32.27
Last Login: Dec 07, 2007 12:47

Device Information:
Device Name: ksx2
IP Address: 192.168.60.110
Firmware: 1.0.0.5.6330

Port States:
10 Ports up
6 Ports down
16 Ports idle

Connected Users:
admin (192.168.32.27)
3 min idle

Favorite Devices:
NewJersey_RemoteOffice_KSX
Sydney_RemoteOffice_KSX

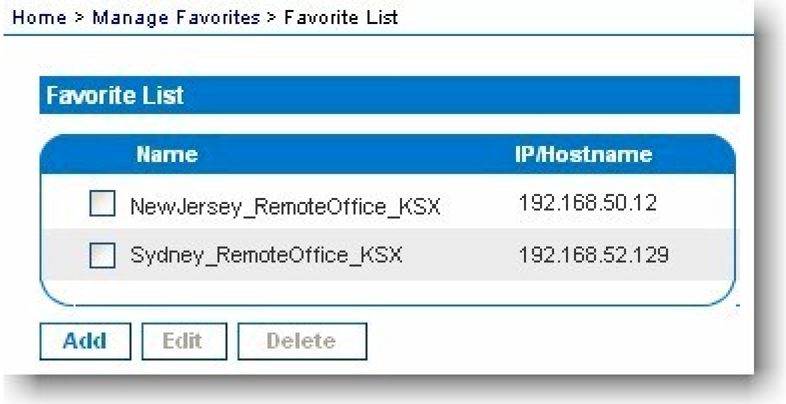
Copyright © 2007 Raritan Computer Inc.

Favorites List

From the Favorites List page, you can add, edit, and delete devices from your list of favorites.

➢ ***To open the Favorites List page:***

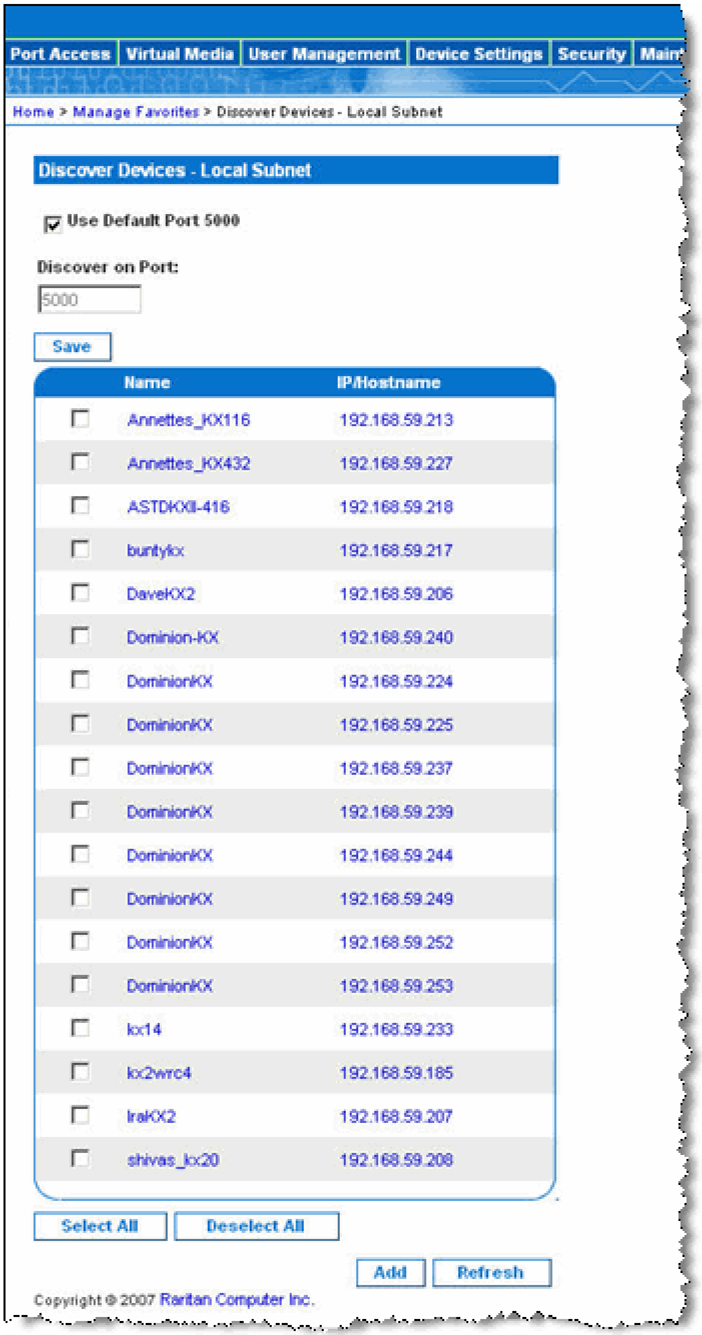
- Choose Manage > Favorites List. The Favorites List page opens.



	Name	IP/Hostname
□	NewJersey_RemoteOffice_KSX	192.168.50.12
□	Sydney_RemoteOffice_KSX	192.168.52.129

Discover Devices - Local Subnet

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



Discover Devices - Local Subnet

☑ Use Default Port 5000

Discover on Port: 5000

	Name	IP/Hostname
□	Annettes_KX116	192.168.59.213
□	Annettes_KX432	192.168.59.227
□	ASTDKXII-416	192.168.59.218
□	buntykx	192.168.59.217
□	DaveKX2	192.168.59.206
□	Dominion-KX	192.168.59.240
□	DominionKX	192.168.59.224
□	DominionKX	192.168.59.225
□	DominionKX	192.168.59.237
□	DominionKX	192.168.59.239
□	DominionKX	192.168.59.244
□	DominionKX	192.168.59.249
□	DominionKX	192.168.59.252
□	DominionKX	192.168.59.253
□	kx14	192.168.59.233
□	kx2wrc4	192.168.59.185
□	IraKX2	192.168.59.207
□	shivas_kx20	192.168.59.208

Copyright © 2007 Raritan Computer Inc.

➢ *To discover devices on the local subnet:*

1. Choose Favorites > Discover Devices - Local Subnet. The Discover Devices - Local Subnet page opens.
2. Choose the appropriate discovery port (refer to ***Network Miscellaneous Settings*** (on page 222) for information about the discovery port):
   - To use the default discovery port, select the Use Default Port 5000 option.
   - To use a different discovery port:

   a. Deselect the Use Default Port 5000 option.

   b. Type the port number into the Discover on Port field.

   c. Click Save.
3. Click Refresh. The list of devices on the local subnet is refreshed.

➢ *To add devices to your Favorites List:*

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

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

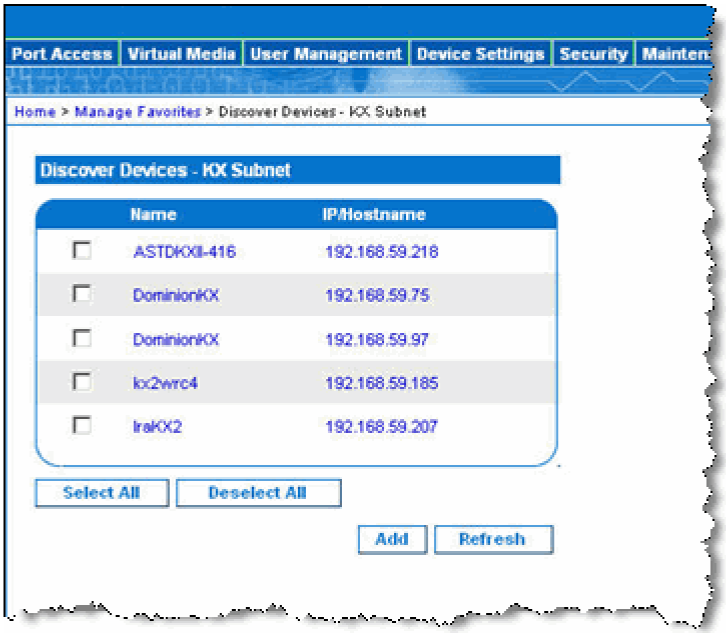
➢ *To access a discovered device:*

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

Discover Devices - KX Subnet

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

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



	Name	IP/Hostname
□	ASTDKXII-416	192.168.59.218
□	DominionKX	192.168.59.75
□	DominionKX	192.168.59.97
□	kx2wrc4	192.168.59.185
□	IraKX2	192.168.59.207

➢ To discover devices on the device subnet:

1. Choose Favorites > Discover Devices - Dominion KX II Subnet. The Discover Devices - Dominion KX II Subnet page opens.
2. Click Refresh. The list of devices on the local subnet is refreshed.

➢ To add devices to your Favorites List:

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

Tip: Use the Select All and Deselect All buttons to quickly select all (or deselect all) devices in the Dominion KX II device subnet.

➢ To access a discovered device:

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

Add New Favorite

➢ To add a device to your favorites list:

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

➢ To delete a favorite:

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

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

➢ To edit a favorite:

1. From the Favorites List page, select the checkbox next to the appropriate Dominion KX II device.
2. Click the Edit button. The Edit page opens.
3. Update the fields as necessary:
   - Description. Enter something meaningful.
   - IP Address. Type the IP Address of the Dominion KX II unit.
   - Port. Change the discovery Port (if necessary).
4. Click OK.

Logging off

➢ To quit the Dominion KX II Remote Console:

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

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

Multi-Platform Client Interface

See ***Multi-Platform Client (MPC)*** (on page 86) for information on using the Multi-Platform Client.

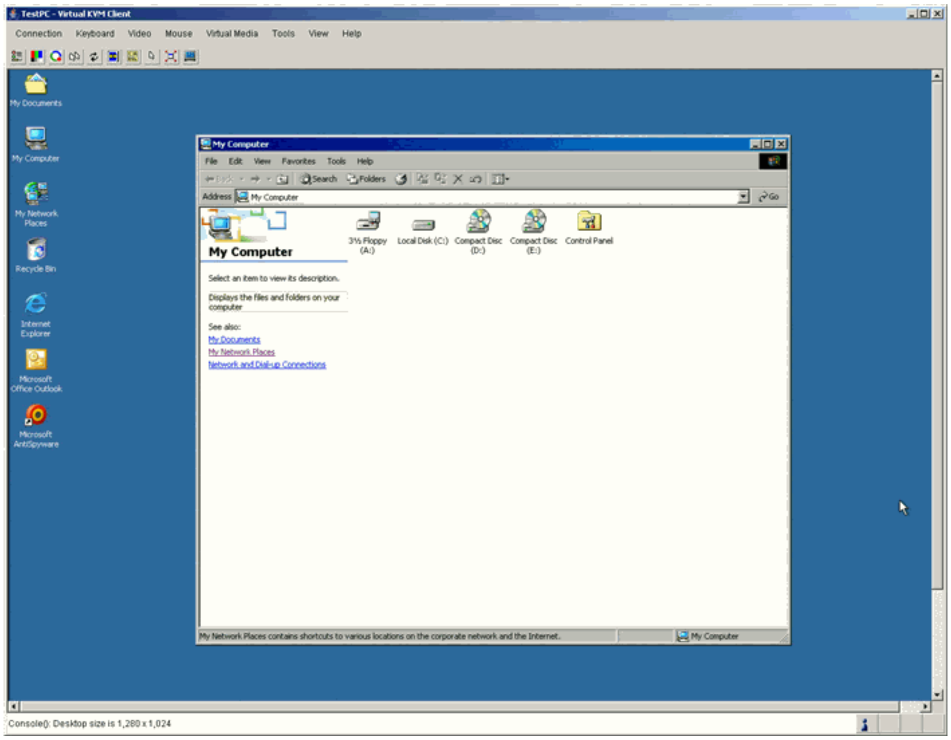
Virtual KVM Client

Overview

Whenever you access a target server using the Dominion KX II Remote Console, a Virtual KVM Client (VKC) window is opened. There is one Virtual KVM Client for each target server connected to; these windows can be accessed via the Windows task bar.

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

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



Console(): Desktop size is 1,280 x 1,024

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

Feature	Description
Menu bar	Drop-down menus of commands and settings.
Toolbar	Shortcut buttons to frequently used features and commands.
Target server video window	Target device display.
Status bar	Real-time information on connection parameters, target server window size, concurrent connections, Caps Lock indicator, and Num Lock indicator.

Connecting to a KVM Target Server

➢ ***To connect to a KVM target server:***

1. From the Dominion KX II Remote Console, click the Port Access tab to open it. The Port Access page opens.
2. Click the Port Name of the target you want to access. The Port Action menu is displayed.
3. Click Connect. A ***Virtual KVM Client*** (on page 50) window opens to the target server connected to that port.

Switching Between KVM Target Servers

With the Dominion KX II, you can access several KVM target servers. Dominion KX II provides the ability to switch from one target server to another.

Note: This feature is available in the Dominion KX II Remote Console only.

➢ ***To switch between KVM target servers:***

1. While already using a target server, access the Dominion KX II Port Access page.
2. Click the port name of the target you want to access. The Port Action menu is displayed.
3. Choose Switch From from the Port Action menu. The Virtual KVM Client window switches to the new target server you selected.

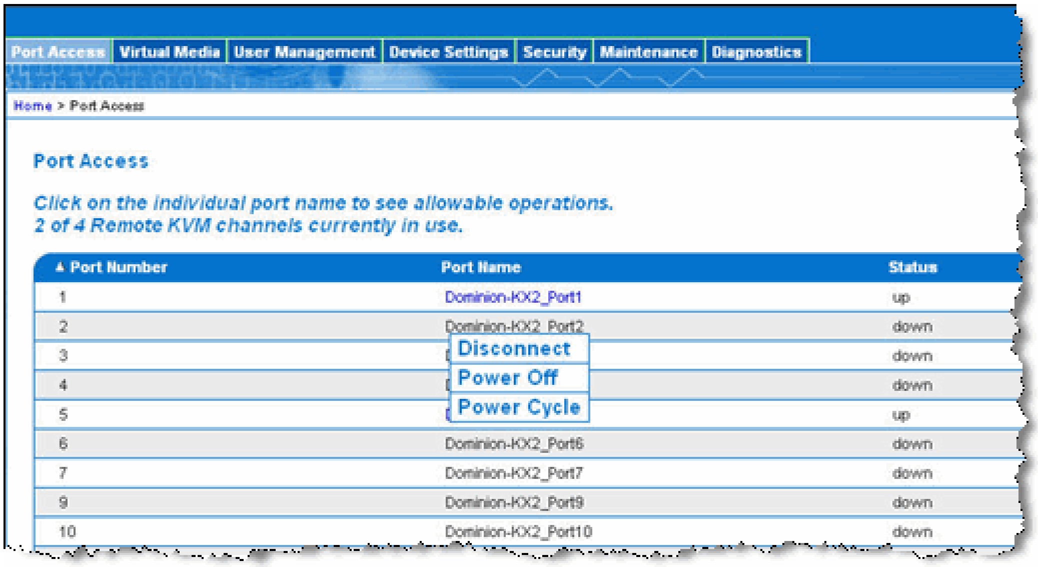
Power Controlling a Target Server

Note: These features are available only when you have made power associations. Refer to *Power Control* (on page 236) for more information.

Power Cycle a Target Server

➢ ***To power cycle a KVM target server:***

1. From the Dominion KX II Remote Console, click the Port Access tab to open it. The Port Access page opens.
2. Click the Port Name of the appropriate target server. The Port Action menu is displayed.



Port Access

Click on the individual port name to see allowable operations.
2 of 4 Remote KVM channels currently in use.

▲ Port Number	Port Name	Status
1	Dominion-KX2_Port1	up
2	Dominion-KX2_Port2	down
3	[illegible]	down
4	[illegible]	down
5	[illegible]	up
6	Dominion-KX2_Port6	down
7	Dominion-KX2_Port7	down
9	Dominion-KX2_Port9	down
10	Dominion-KX2_Port10	down

3. Choose Power Cycle. A message is displayed confirming the action taken.

Power On a Target Server

➢ ***To power on a target server:***

1. From the Dominion KX II Remote Console, click the Port Access tab to open it. The Port Access page opens.
2. Click the port name of the appropriate target server. The Port Action menu is displayed.
3. Choose Power On. A message is displayed confirming the action taken.

Power Off a Target Server

➢ ***To power off a target server:***

1. From the Dominion KX II Remote Console, click the Port Access tab to open it. The Port Access page opens.
2. Click the port name of the appropriate target server. The Port Action menu is displayed.
3. Choose Power Off. A message is displayed confirming the action taken.

Disconnecting KVM Target Servers

Note: This item is not available on the Dominion KX II Local Console; the only way to disconnect from the switched target in the Local Console is to use the hot key.

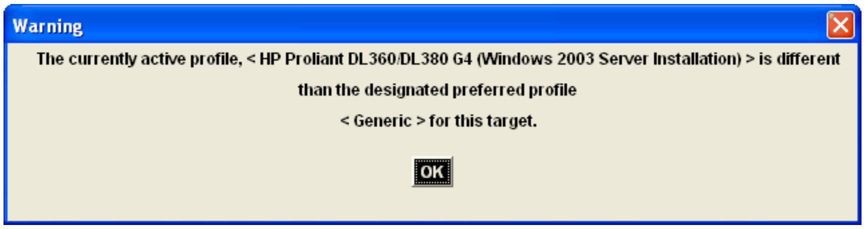
➢ ***To disconnect a target server:***

1. Click the port name of the target you want to disconnect. The Port Action menu is displayed.
2. Choose Disconnect on the Port Action menu.

Tip: You can also close the Virtual KVM Client window by selecting Connection > Exit from the Virtual KVM menu.

Choosing USB Profiles

When you connect to a KVM target server for the first time, as described in ***Connecting to a KVM Target Server*** (on page 51), the preferred USB profile for the port is automatically used. If you have connected to the target server previously using a different profile, the USB profile from the last connection is used. You are alerted to the use of a profile other than the preferred profile by a warning like the following:



Warning

The currently active profile, < HP Proliant DL360/DL380 G4 (Windows 2003 Server Installation) > is different than the designated preferred profile < Generic > for this target.

After you have connected to a target server, you can change the USB profile as necessary. By default, the profiles that appear under the USB Profile menu in the VKC are those that you are most likely to use. These profiles have been preselected by the administrator for use with the connected target server depending on your operational requirements. However, all profiles are available to be selected.

➢ ***To choose a USB profile:***

1. Connect to a KVM target server as described in ***Connecting to a KVM Target Server*** (on page 51).
2. In VKC, choose a USB profile from the USB Profile menu.

   The name of the profile indicates the operating system or server it should be used with. For more detailed information about a USB profile, see ***Configuring USB Profiles*** (on page 185).

Using the VKC

Menu Tree

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

- Connection menu:
  - Properties
  - Connection Info
  - Exit
- Keyboard menu:
  - Send Ctrl + Alt + Delete
  - CIM Keyboard/Mouse Options
  - Keyboard Macros
  - Keyboard Mouse Options
  - User-Created Macros **Optional**
- Video menu:
  - Refresh Screen
  - Auto-Sense Video Settings
  - Calibrate Color

  - Video Settings
- Mouse menu:
  - Synchronize Mouse
  - Single Mouse Cursor
  - Absolute
  - Intelligent
  - Standard
- Virtual Media menu:
  - Connect Drive
  - Connect CD-ROM/ISO Image
- Tools menu:
  - Options
- View menu:
  - View Toolbar
  - Scaling
  - Target Screen Resolution
- Help menu:
  - About Raritan Virtual KVM Client

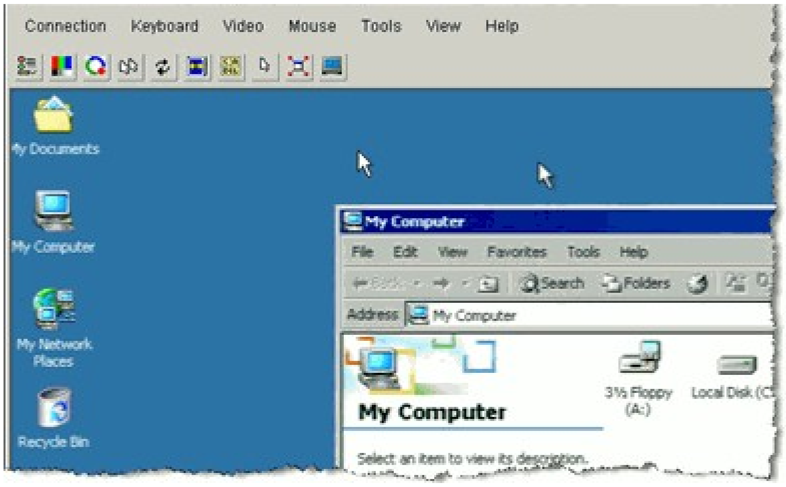
VKC Toolbar

Button	Description
☰	Properties
▥	Video settings
○	Calibrate color
⇖	Synchronize the target mouse cursor
⟳	Refresh screen
↔	Auto-sense video
C A DEL	Send Ctrl+Alt+Delete
⇖	Single mouse cursor
⤢	Full screen

Button	Description
🖥	Resize video to fit screen

Mouse Pointer Synchronization

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



On fast LAN connections, you may want to disable the Virtual KVM Client mouse pointer and view only the target server's pointer. You can toggle between these two modes (single mouse and dual mouse).

Mouse Synchronization Tips

Be sure to follow these steps when configuring mouse synchronization:

1. Verify that the selected video resolution and refresh rate is among those supported by the Dominion KX II device. The Virtual KVM Client Connection Info dialog displays the actual values that the Dominion KX II is seeing. Refer to ***Supported Video Resolutions*** (on page 288) for more information about the video resolutions that are supported.
2. Verify that the cable length is within the specified limits for the selected video resolution. Refer to ***Target Server Connection Distance and Video Resolution*** (on page 299) for more information.

3. Verify that the mouse and video have been properly configured during the installation process. Refer to ***Installation and Configuration*** (on page 10) for complete instructions.
4. Force an auto-sense by clicking the "Virtual KVM Client auto-sense" button.
5. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris KVM target servers):
   a. Open a terminal window.
   b. Enter the `xset mouse 1 1 command`.
   c. Close the terminal window.
6. Click the "Virtual KVM Client mouse synchronization" button .

Additional Notes for Intelligent Mouse Mode

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

Synchronize Mouse

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

➢ ***To synchronize the mouse, do one of the following:***

- Choose Mouse > Synchronize Mouse.
- Click the Synchronize Mouse button in the toolbar.

Mouse Synchronization Tips

Be sure to follow these steps when configuring mouse synchronization:

1. Verify that the selected video resolution and refresh rate is among those supported by the Dominion KX II device. The Virtual KVM Client Connection Info dialog displays the actual values that the Dominion KX II is seeing. Refer to ***Supported Video Resolutions*** (on page 288) for more information about the video resolutions that are supported.
2. Verify that the cable length is within the specified limits for the selected video resolution. Refer to ***Target Server Connection Distance and Video Resolution*** (on page 299) for more information.

3. Verify that the mouse and video have been properly configured during the installation process. Refer to ***Installation and Configuration*** (on page 10) for complete instructions.
4. Force an auto-sense by clicking the "Virtual KVM Client auto-sense" button.
5. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris KVM target servers):
    a. Open a terminal window.
    b. Enter the `xset mouse 1 1 command`.
    c. Close the terminal window.
6. Click the "Virtual KVM Client mouse synchronization" button .

Additional Notes for Intelligent Mouse Mode

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

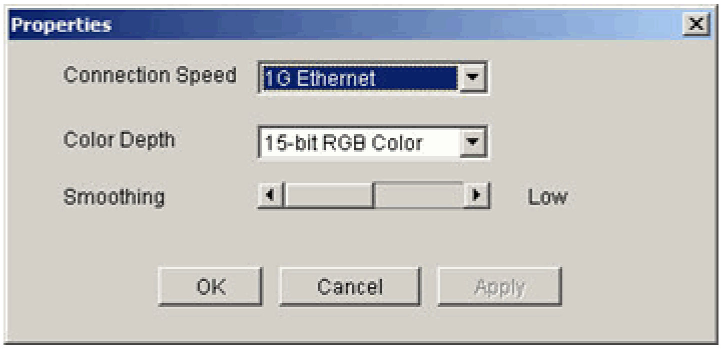
Connection Properties

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

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

➢ *To set the connection properties:*

1. Choose Connection > Properties or click the Connection Properties button in the toolbar. The Properties dialog opens.



Properties

Connection Speed: 1G Ethernet

Color Depth: 15-bit RGB Color

Smoothing: Low

2. Choose the Connection Speed from the drop-down list. The Dominion KX II can automatically detect available bandwidth and not limit bandwidth use; but you can also adjust this usage according to bandwidth limitations.
   - Auto
   - 1G Ethernet
   - 100 Mb Ethernet
   - 10 Mb Ethernet
   - 1.5 Mb (MAX DSL/T1)
   - 1 Mb (Fast DSL/T1)
   - 512 Kb (Medium DSL/T1)
   - 384 Kb (Slow DSL/T1)
   - 256 Kb (Cable)
   - 128 Kb (Dual ISDN)

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

3. Choose the Color Depth from the drop-down list. The Dominion KX II can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths.
   - 15-bit RGB Color
   - 8-bit RGB Color
   - 4-bit Color
   - 4-bit Gray
   - 3-bit Gray
   - 2-bit Gray
   - Black and White

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

4. Use the slider to select the desired level of Smoothing (15-bit color mode only). The level of smoothing determines how aggressively to blend screen regions with small color variation into a single smooth color. Smoothing improves the appearance of target video by reducing displayed video noise.
5. Click OK to set these properties.

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

- Choose Connection > Exit.

Properties Dialog

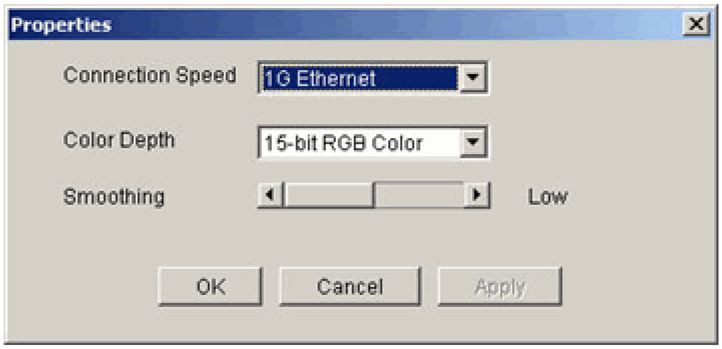
The Dominion KX II dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. The Dominion KX II units optimize KVM output not only for LAN use, but also for WAN use. These units can also control color depth and limit video output, offering an optimal balance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

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

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

➢ ***To set the connection properties:***

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



Connection Speed: 1G Ethernet

Color Depth: 15-bit RGB Color

Smoothing: Low

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

   Auto

   1G Ethernet

   100 Mb Ethernet

   10 Mb Ethernet

   1.5 Mb (MAX DSL/T1)

   1 Mb (Fast DSL/T1)

   512 Kb (Medium DSL/T1)

   384 Kb (Slow DSL/T1)

   256 Kb (Cable)

128 Kb (Dual ISDN)

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

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

   15-bit RGB Color

   8-bit RGB Color

   4-bit Color

   4-bit Gray

   3-bit Gray

   2-bit Gray

   Black and White

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

4. Use the slider to select the desired level of Smoothing (15-bit color mode only). The level of smoothing determines how aggressively to blend screen regions with small color variation into a single smooth color. Smoothing improves the appearance of target video by reducing displayed video noise.
5. Click OK to set these properties.

Connection Information

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

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

The following information is displayed about the current connection:

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

➢ ***To copy this information:***

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

Exit

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

- Choose Connection > Exit.

Keyboard Options

Send Ctrl+Alt+Delete

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

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

➢ ***To send a Ctrl+Alt+Delete key sequence to the target server,***

- Choose Keyboard > Send Ctrl+Alt+Delete or click the Send Ctrl+Alt+Delete button C A DEL in the toolbar.

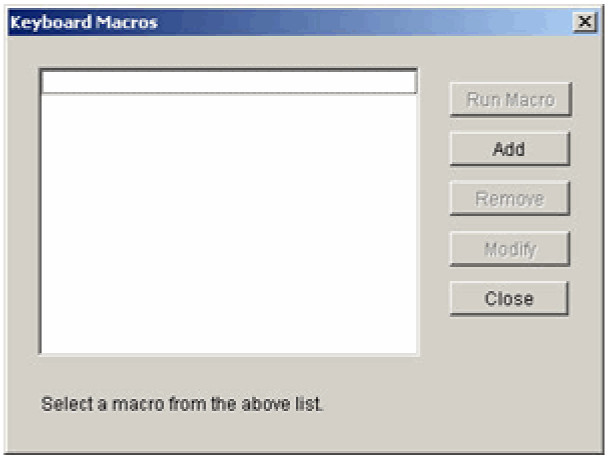
Keyboard Macros

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

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

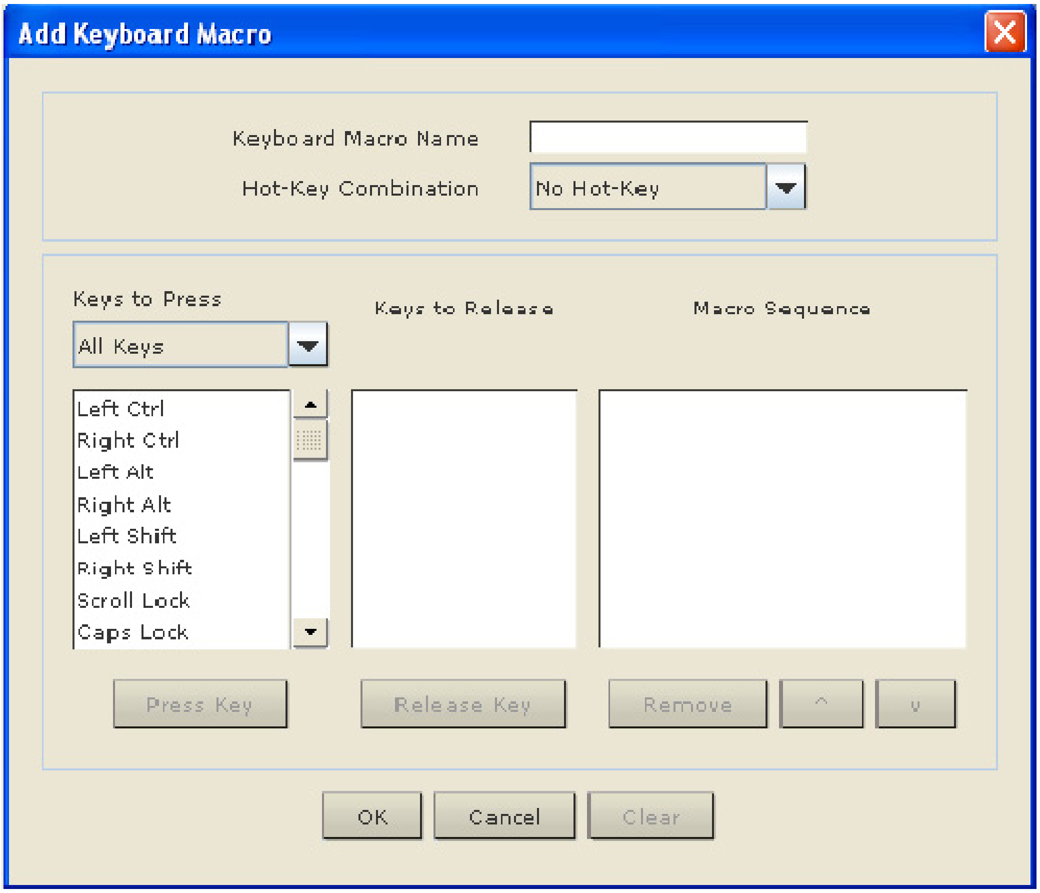
➢ ***To create a keyboard macro (add a macro):***

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.



Select a macro from the above list.

2. Click Add. The Add Keyboard Macro dialog appears.



3. Type a name in the Keyboard Macro Name field. This is the name that will display on the Virtual KVM Client menu bar after the macro is created. In this example, Minimize All Windows is used.

4. In the Keys to Press drop-down list:

   a. Scroll through and select each key for which you would like to emulate a key press (in the order in which they are to be pressed).

   b. Click the Press Key button after each selection. As each key is selected, it displays in the Keys to Release field.

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

5. In the Keys to Release field:

   a. Choose each key for which you would like to emulate a key release (in the order in which they are to be released).

   b. Click Release Key after each selection.

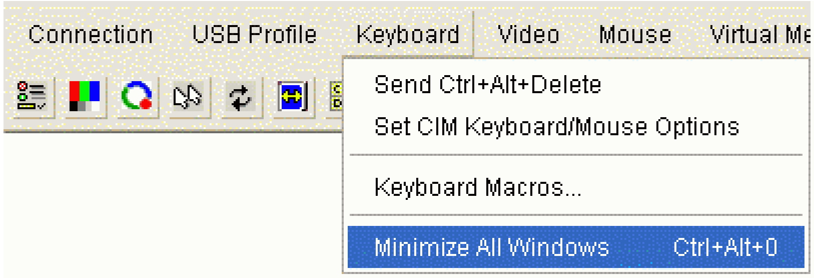
In this example, both keys pressed must also be released.

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

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

7. Click OK in the Add Keyboard Macro dialog to save the macro.

8. Click Close from the Keyboard Macros dialog. The keyboard macro is now listed as a command in the Keyboard menu.



➢ *To clear all fields and start over:*

- Click the Clear button.

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

➢ *To execute a macro (using the example outlined in this guide):*

- Choose Keyboard > Minimize All Windows.

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

➢ *To execute a macro:*

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.

2. Select the macro from among those listed.

3. Click Run Macro.

➢ *To modify a macro:*

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.

2. Choose the macro from among those listed.
3. Click Modify. The Add/Edit Macro dialog appears.
4. Make your changes.
5. Click OK.

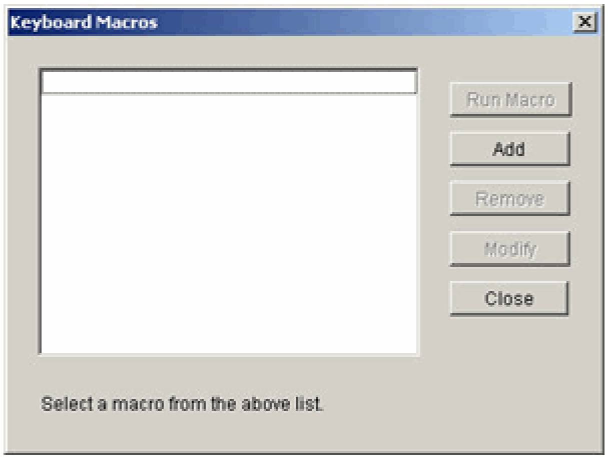
➢ ***To remove a macro:***

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

Creating a Keyboard Macro

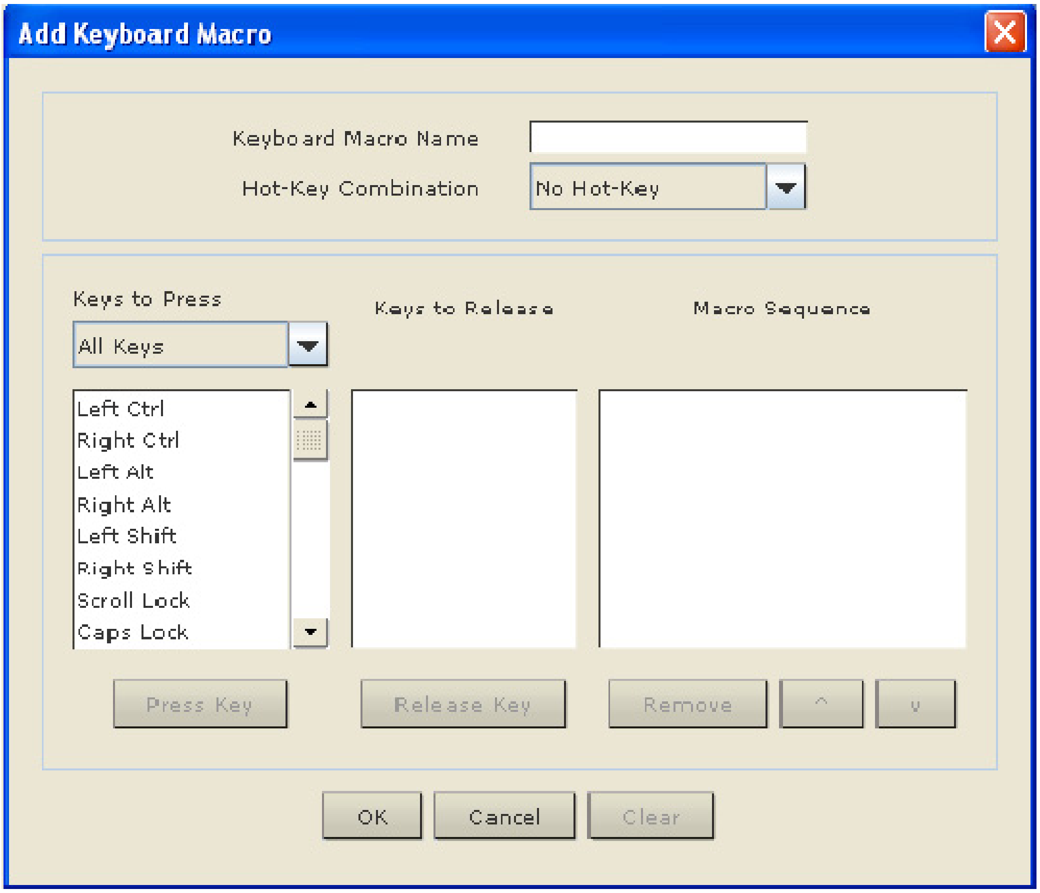
➢ ***To create a keyboard macro (add a macro):***

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.



Select a macro from the above list.

2. Click Add. The Add Keyboard Macro dialog appears.



3. Type a name in the Keyboard Macro Name field. This is the name that will display on the Virtual KVM Client menu bar after the macro is created. In this example, Minimize All Windows is used.

4. In the Keys to Press drop-down list:

   a. Scroll through and select each key for which you would like to emulate a key press (in the order in which they are to be pressed).

   b. Click the Press Key button after each selection. As each key is selected, it displays in the Keys to Release field.

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

5. In the Keys to Release field:

   a. Choose each key for which you would like to emulate a key release (in the order in which they are to be released).

   b. Click Release Key after each selection.

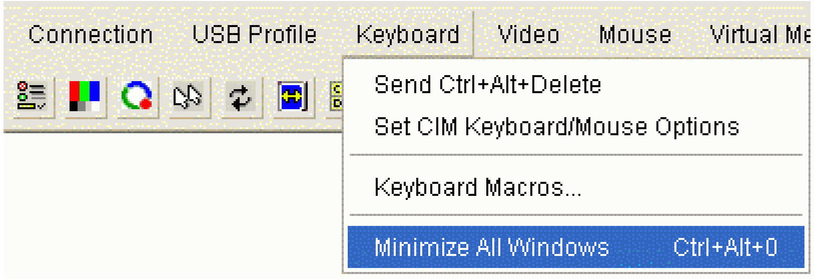
In this example, both keys pressed must also be released.

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

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

7. Click OK in the Add Keyboard Macro dialog to save the macro.

8. Click Close from the Keyboard Macros dialog. The keyboard macro is now listed as a command in the Keyboard menu.



➢ ***To clear all fields and start over:***

- Click the Clear button.

Running a Keyboard Macro

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

➢ ***To execute a macro (using the example outlined in this guide):***

- Choose Keyboard > Minimize All Windows.

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

➢ ***To execute a macro:***

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

Modifying a Keyboard Macro

➢ ***To modify a macro:***

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

Removing a Keyboard Macro

➢ ***To remove a macro:***

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

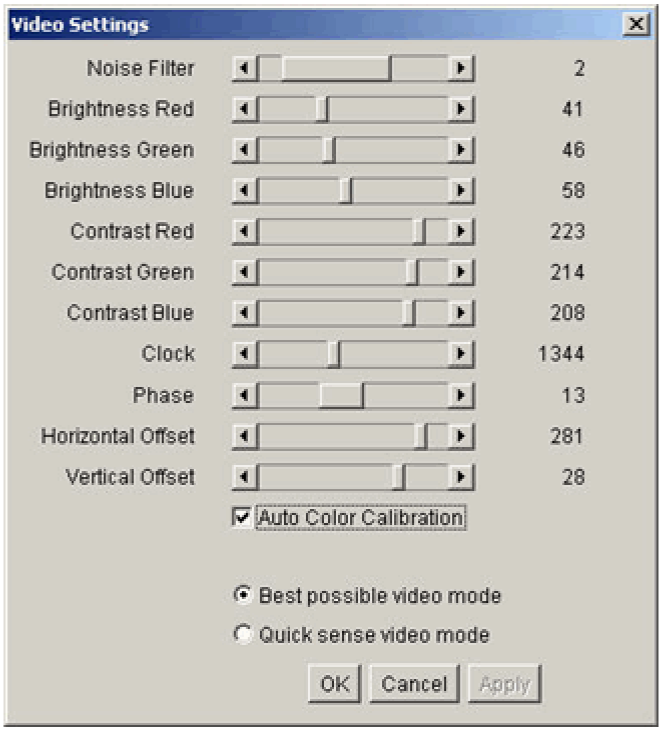
Video Properties

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

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

➢ *To change the video settings manually:*

1. Choose Video > Video Settings or click the Video Setting button in the toolbar. The Video Settings dialog appears displaying the current settings:



Video Settings

Noise Filter	2
Brightness Red	41
Brightness Green	46
Brightness Blue	58
Contrast Red	223
Contrast Green	214
Contrast Blue	208
Clock	1344
Phase	13
Horizontal Offset	281
Vertical Offset	28

☑ Auto Color Calibration

● Best possible video mode

○ Quick sense video mode

2. Use the sliders to adjust the settings to achieve the desired results (as you adjust the settings, the effects are immediately visible):

- Noise Filter - The Dominion KX II can filter out the electrical interference of video output from graphics cards. This feature optimizes picture quality and reduces bandwidth. Higher settings transmit variant pixels only if a large color variation exists in comparison to the neighboring pixels. However, setting the threshold too high can result in the unintentional filtering of desired screen changes.
  Lower settings transmit most pixel changes. Setting this threshold too low can result in higher bandwidth use.
- Brightness - Use this setting to adjust the brightness of the target server display.
  - Red - Controls the brightness of the red signal.
  - Green - Controls the brightness of the green signal.
  - Blue - Controls the brightness of the blue signal.
- Color Contrast Settings - Controls the contrast adjustment.
  - Contrast Red - Controls the red signal.
  - Contrast Green - Controls the green signal.
  - Contrast Blue - Controls the blue signal.
- If the video image looks extremely blurry or unfocused, the settings for clock and phase can be adjusted until a better image appears on the active target server.

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

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

        - Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor.
        - Vertical Offset - Controls the vertical positioning of the target server display on your monitor.
    - Auto Color Calibration - Check this option if you would like automatic color calibration.
    - Video Sensing - Select the video sensing mode:
        - Best possible video mode - The Dominion KX II will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.
        - Quick sense video mode - With this option, the Dominion KX II will use Quick Video Auto Sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.

3. Click Apply. The Video Settings are changed.

Refresh Screen

The Refresh Screen command forces a refresh of the video screen. Video settings can be refreshed automatically in several ways:

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

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

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

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

Auto-Sense Video Settings

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

➢ ***To automatically detect the video settings, do one of the following:***

- Choose Video > Auto-sense Video Settings or click the Auto-Sense Video Settings button from toolbar. A message opens stating that the auto adjustment is in progress.

Calibrate Color

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

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

➢ ***To calibrate the color, do one of the following:***

- Choose Video > Calibrate Color or click the Calibrate Color button . The target device screen updates its color calibration.

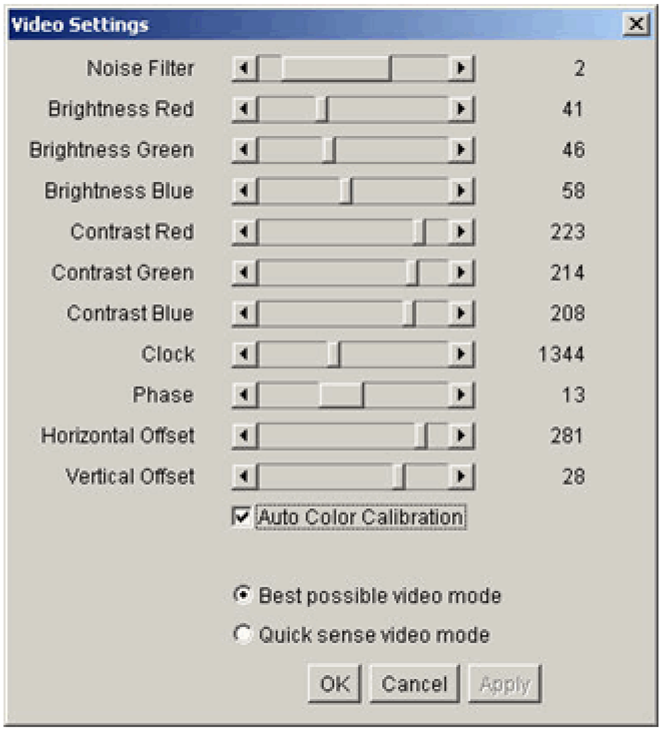
Video Settings

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

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

➢ *To change the video settings:*

1. Choose Video > Video Settings. The Video Settings dialog appears displaying the current settings:



Noise Filter	2
Brightness Red	41
Brightness Green	46
Brightness Blue	58
Contrast Red	223
Contrast Green	214
Contrast Blue	208
Clock	1344
Phase	13
Horizontal Offset	281
Vertical Offset	28

☑ Auto Color Calibration

● Best possible video mode

○ Quick sense video mode

2. Use the sliders to adjust the settings to achieve the desired results (as you adjust the settings the effects are immediately visible):

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

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

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

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

3. Click Apply. The Video Settings are changed.

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

Mouse Options

When controlling a target server, the Dominion KX II Remote Console displays two mouse cursors: one belonging to your client workstation and the other belonging to the target server.

You can operate in either single mouse mode or dual mouse mode. When in dual mouse mode and provided the option is properly configured, the mouse cursors will align. If you experience difficulty with mouse synchronization, refer to ***Step 3: Configure KVM Target Servers*** (on page 21).

When there are two mouse cursors, the Dominion KX II device offers several mouse modes:

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

Synchronize Mouse

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

➢ ***To synchronize the mouse, do one of the following:***

- Choose Mouse > Synchronize Mouse.
- Click the Synchronize Mouse button in the toolbar.

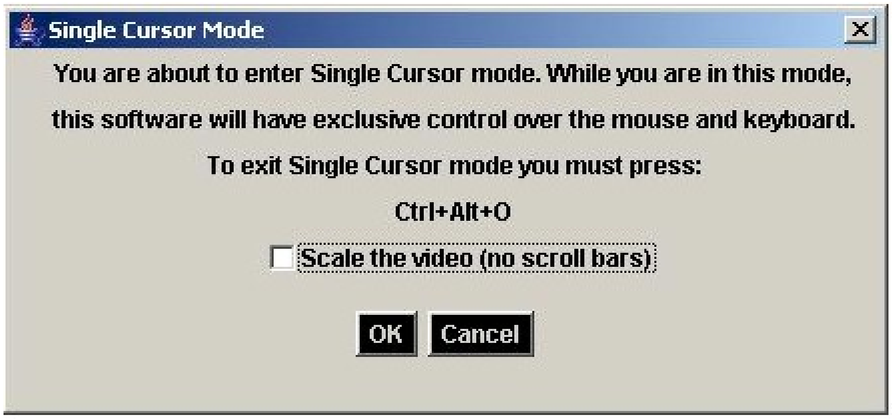
Single Mouse Cursor

Single Mouse mode uses only the target server mouse cursor and the local mouse pointer no longer appears onscreen. While in single mouse mode, the Synchronize Mouse command is not available (there is no need to synchronize a single mouse cursor).

➢ ***To enter single mouse mode, do one of the following:***

1. Choose Mouse > Single Mouse Cursor.

2. Click the Single/Double Mouse Cursor button in the toolbar.



Single Cursor Mode

You are about to enter Single Cursor mode. While you are in this mode, this software will have exclusive control over the mouse and keyboard.

To exit Single Cursor mode you must press:

Ctrl+Alt+O

□ Scale the video (no scroll bars)

➤ ***To exit single mouse mode:***

1. When entering single mouse mode, the following message is displayed. Click OK.
2. Press Ctrl+Alt+O on your keyboard to exit single mouse mode.

Standard Mouse Mode

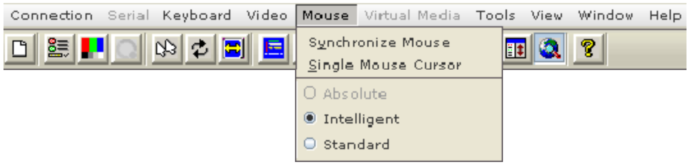
Standard Mouse mode uses a standard mouse synchronization algorithm using relative mouse positions. Standard Mouse mode requires that mouse acceleration is disabled and other mouse parameters are set correctly in order for the client and server mouse to stay synchronized. Standard Mouse mode is the default.

➤ ***To enter standard mouse mode:***

- Choose Mouse > Standard.

Intelligent Mouse Mode

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



➢ *To enter intelligent mouse mode:*

- Choose Mouse > Intelligent.

Intelligent Mouse Synchronization Conditions

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

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

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

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

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

Absolute Mouse Mode

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

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

➢ ***To enter absolute mouse mode:***

- Choose Mouse > Absolute.

VKC Virtual Media

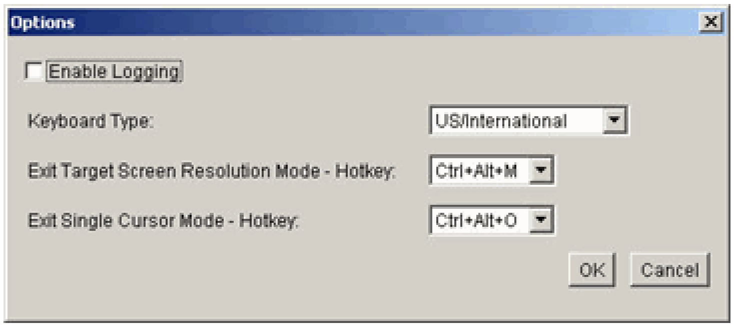
Refer to the chapter on Virtual Media for complete information about setting up and using virtual media.

Tool Options

From the Tools menu, you can specify certain options for use with the Virtual KVM Client. Specifically, you are able to enable logging, set the keyboard type, and define hot keys for exiting target screen resolution mode and single cursor mode.

➢ ***To set the tools options:***

1. Choose Tools > Options. The Options dialog appears.



Options

☐ Enable Logging

Keyboard Type: US/International

Exit Target Screen Resolution Mode - Hotkey: Ctrl+Alt+M

Exit Single Cursor Mode - Hotkey: Ctrl+Alt+O

2. Select the Enable Logging checkbox only if directed to by Technical Support. This option creates a log file in your home directory.
3. Choose the Keyboard Type from the drop-down list (if necessary). The options include:
   - US/International
   - French (France)

- German (Germany)
- Japanese
- United Kingdom
- Korean (Korea)
- Belgian
- Norwegian
- Danish
- Swedish

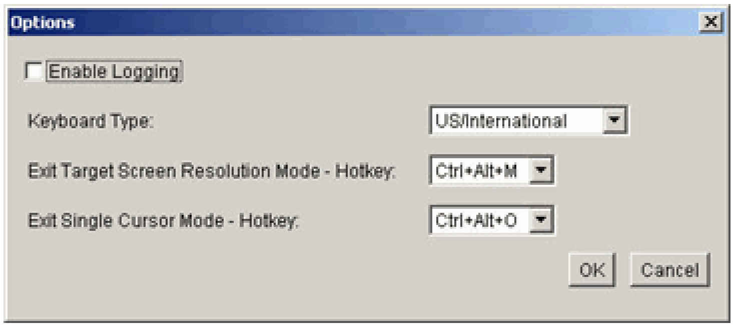
4. Exit Target Screen Resolution Mode - Hotkey. When you enter target screen resolution mode, the display of the target server becomes full screen and acquires the same resolution as the target server. This is the hot key used for exiting this mode.
5. Exit Single Cursor Mode - Hotkey. When you enter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

Options

From the Tools menu, you can specify certain options for use with the Virtual KVM Client. Specifically, you are able to enable logging, set the keyboard type, and define hot keys for exiting target screen resolution mode and single cursor mode.

➢ ***To set the tools options:***

1. Choose Tools > Options. The Options dialog appears.



Options

☐ Enable Logging

Keyboard Type: US/International

Exit Target Screen Resolution Mode - Hotkey: Ctrl+Alt+M

Exit Single Cursor Mode - Hotkey: Ctrl+Alt+O

2. Select the Enable Logging checkbox only if directed to by Technical Support. This option creates a log file in your home directory.

3. Choose the Keyboard Type from the drop-down list (if necessary). The options include:
    - US/International
    - French (France)
    - German (Germany)
    - Japanese
    - United Kingdom
    - Korean (Korea)
    - Belgian
    - Norwegian
    - Danish
    - Swedish
4. Exit Target Screen Resolution Mode - Hotkey. When you enter target screen resolution mode, the display of the target server becomes full screen and acquires the same resolution as the target server. This is the hot key used for exiting this mode; select from the drop-down list.
5. Exit Single Cursor Mode - Hotkey. When you enter single cursor mode, only the target server mouse cursor is visible. This is the hot key used to exit single cursor mode and bring back the client mouse cursor; select from the drop-down list.
6. Click OK.

View Options

View Toolbar

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

➢ ***To toggle the display of the toolbar (on and off):***

- Choose View > View Toolbar.

Scaling

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

➢ ***To toggle scaling (on and off):***

- Choose View > Scaling.

Target Screen Resolution

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

➢ ***To enter target screen resolution:***

- Choose View > Target Screen Resolution.

➢ ***To exit target screen resolution mode:***

- Press the hot key configured in the Tools Options dialog. The default is Ctrl+Alt+M.

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

View Toolbar

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

➢ ***To toggle the display of the toolbar (on and off):***

- Choose View > View Toolbar.

Scaling

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

➢ ***To toggle scaling (on and off):***

- Choose View > Scaling.

Target Screen Resolution

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

➢ ***To enter target screen resolution:***

- Choose View > Target Screen Resolution.

➢ ***To exit target screen resolution mode:***

- Press the hot key configured in the Tools Options dialog. The default is Ctrl+Alt+M.

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

Help Options

About Raritan Virtual KVM Client

This menu command provides version information about the Virtual KVM Client should you require assistance from Raritan Technical Support.

➢ ***To obtain version information:***

- Choose Help > About Raritan Virtual KVM Client.

About Raritan Virtual KVM Client

This menu command provides version information about the Virtual KVM Client should you require assistance from Raritan Technical Support.

➢ ***To obtain version information:***

- Choose Help > About Raritan Virtual KVM Client.

Multi-Platform Client (MPC)

Raritan Multi-Platform Client (MPC) is a graphical user interface for the Raritan product lines, providing remote access to target servers connected to Raritan KVM over IP devices. Non-Windows users must use Raritan Multi-Platform Client and Windows® users running Internet Explorer must use Raritan Remote Client.

Requirements and Installation

MPC Minimum System Requirements

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

- CPU Speed: 1.0 GHz
- RAM: 512 Mbytes

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

MPC Supported Browsers

MPC supports the following browsers:

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

Raritan Multi-Platform Client (MPC) Supported Operating Systems

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

Raritan MPC is compatible with the following platforms:

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

Launching MPC from a Web Browser

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

1. To open MPC from a client running any supported browser, type *http://IP-ADDRESS/mpc* into the address line, where IP-ADDRESS is the IP address of your Raritan device. MPC will open in a new window. Refer to ***MPC Supported Browsers*** (on page 86) for information on MPC supported browsers.

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

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

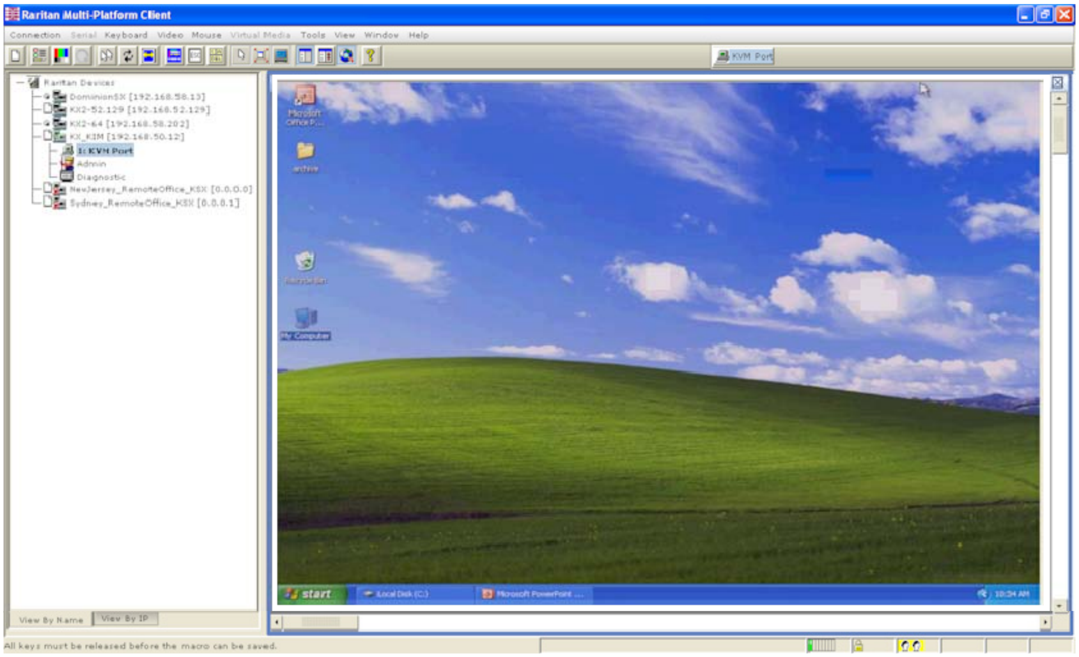
2. If your device is not listed by name in the navigator, add it manually:

   a. Choose Connection > New Profile. The Add Connection window opens.

   b. In the Add Connection window, type a device Description, specify a Connection Type, add the device IP address, and click OK. These specifications can be edited later.

3. In the Navigator panel on the left of the page, double-click the icon that corresponds to your Raritan device to connect to it.

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


Raritan Multi-Platform Client
Connection Serial Keyboard Video Mouse Virtual Media Tools View Window Help
KVM Port
Raritan Devices
DominionSX [192.168.58.13]
KX2-52.129 [192.168.52.129]
KX2-64 [192.168.58.202]
KX_KIM [192.168.50.12]
1: KVM Port
Admin
Diagnostic
NewJersey_RemoteOffice_KSX [0.0.0.0]
Sydney_RemoteOffice_KSX [0.0.0.1]
View By Name
View By IP
Microsoft Office P...
archive
start
Local Disk (C:)
Microsoft PowerPoint ...
10:34 AM

All keys must be released before the macro can be saved.

Special Characters in MPC

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

Character	Description	Character	Description
!	Exclamation point	:	Colon
"	Double quote	;	Semi-colon
#	Pound sign	=	Equal sign
$	Dollar sign	>	Greater than sign
%	Percent sign	?	Question mark
&	Ampersand	@	At sign
'	Single quote	[	Left bracket
(	Left parenthesis	\	Backward slash
)	Right parenthesis	]	Right bracket

Character	Description	Character	Description
*	Asterisk	^	Caret
+	Plus sign	_	Underscore
,	Comma	`	Grave accent
-	Dash	{	Left brace
.	Period	|	Pipe sign
/	Forward slash	}	Right brace
<	Less than sign	~	Tilde

Installing and Opening Standalone MPC

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

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

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

➢ *To check for the MPC JAR file:*

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

Windows

➢ *To check the JRE version in Windows:*

1. Do one of the following to check the JRE version in Windows:
   - Determine your version of the JRE from the Java website: http://www.java.com/en/download/help/testvm.xml.

- Click the Windows Start button at the bottom left of your page and click Control Panel.

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

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

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

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

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

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

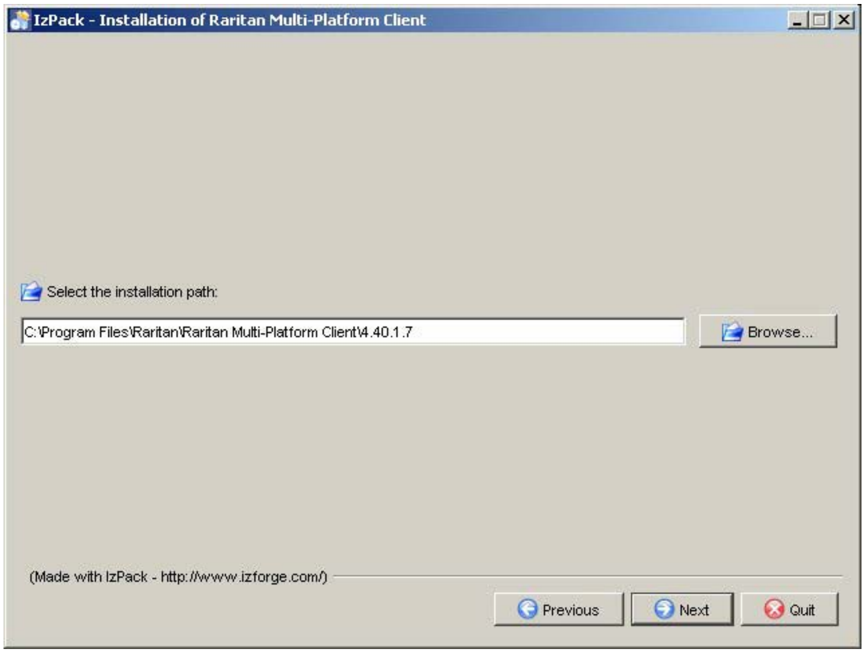
   c. Edit the Path address so that it contains the path to the Java executable.
   For example, if Java is installed on C:\j2re1.4.2_05 and your path is currently set to C:\WINDOWS\SYSTEM32, then change the path to read C:\WINDOWS\SYSTEM32;C:\j2re1.4.2_05

➢ ***To install MPC for Windows:***

1. Download the MPC-installer.jar installation file or copy the file from a known location.

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

3. After the initial dialog appears, click Next.



IzPack - Installation of Raritan Multi-Platform Client

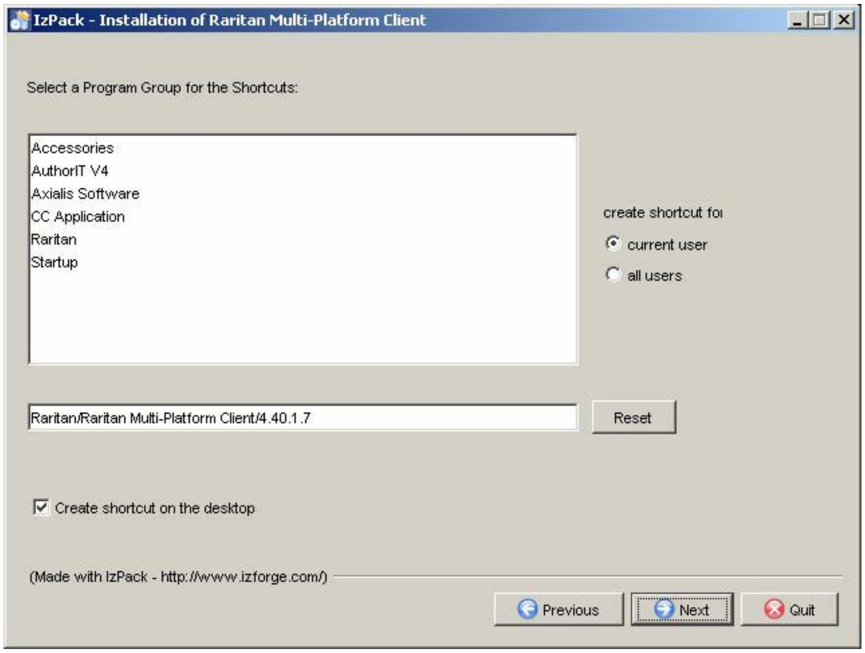
Select the installation path:

C:\Program Files\Raritan\Raritan Multi-Platform Client\4.40.1.7

(Made with IzPack - http://www.izforge.com/)

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

5. Click Next.



IzPack - Installation of Raritan Multi-Platform Client

Select a Program Group for the Shortcuts:

Accessories
AuthorIT V4
Axialis Software
CC Application
Raritan
Startup

create shortcut foı

● current user

○ all users

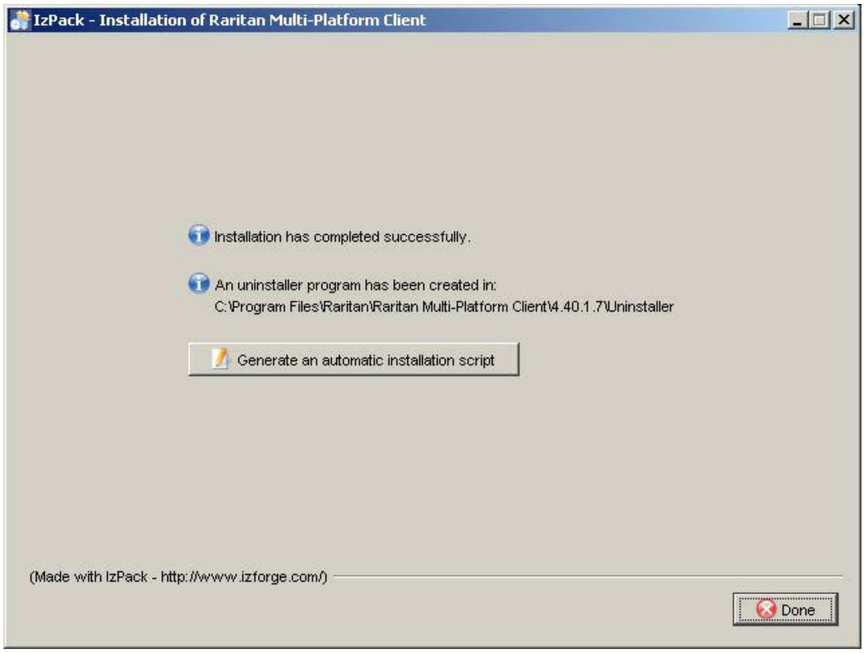
Raritan/Raritan Multi-Platform Client/4.40.1.7

☑ Create shortcut on the desktop

(Made with IzPack - http://www.izforge.com/)

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

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



IzPack - Installation of Raritan Multi-Platform Client

Installation has completed successfully.

An uninstaller program has been created in:
C:\Program Files\Raritan\Raritan Multi-Platform Client\4.40.1.7\Uninstaller

(Made with IzPack - http://www.izforge.com/)

➢ *To open MPC in Windows:*

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

Linux

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

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

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

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

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

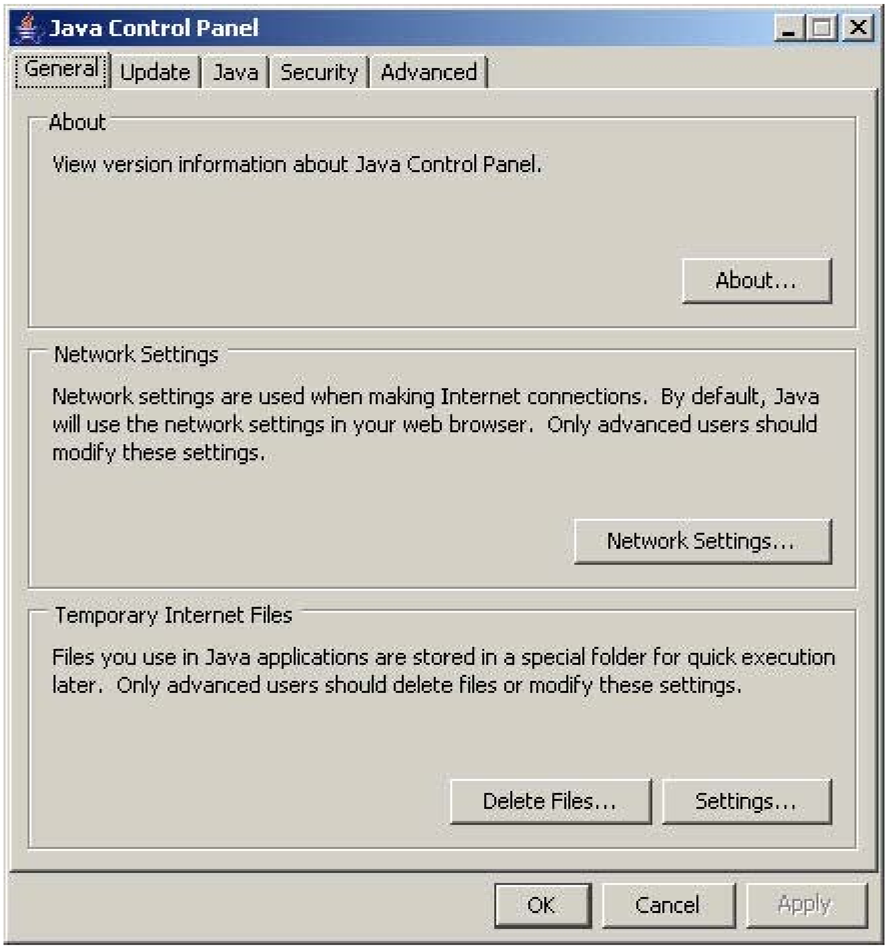
For Linux/UNIX environments, the Java Control Panel is located in the JRE's bin directory; the location varies based on where JRE was installed by your Linux/UNIX administrator.

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

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

1. From the Start menu, click Control Panel.

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



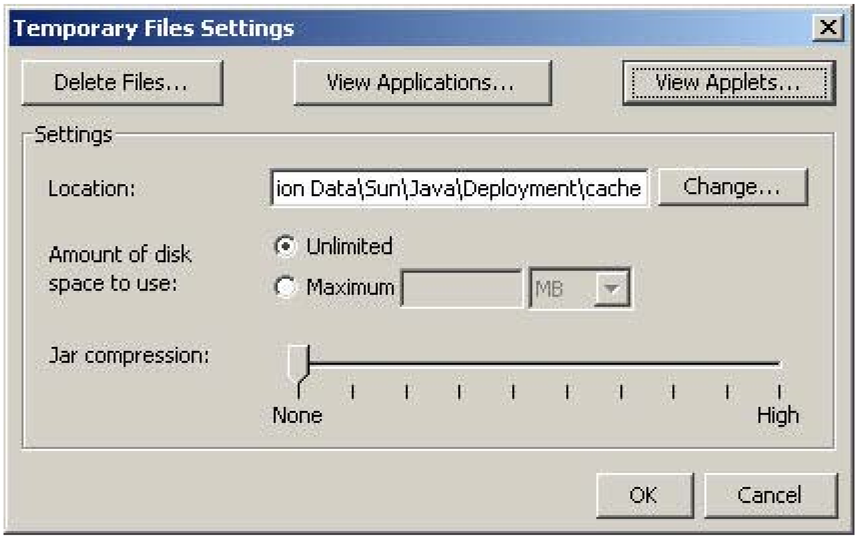
View version information about Java Control Panel.

Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.

Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.

3. To disable Java caching:

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



Temporary Files Settings

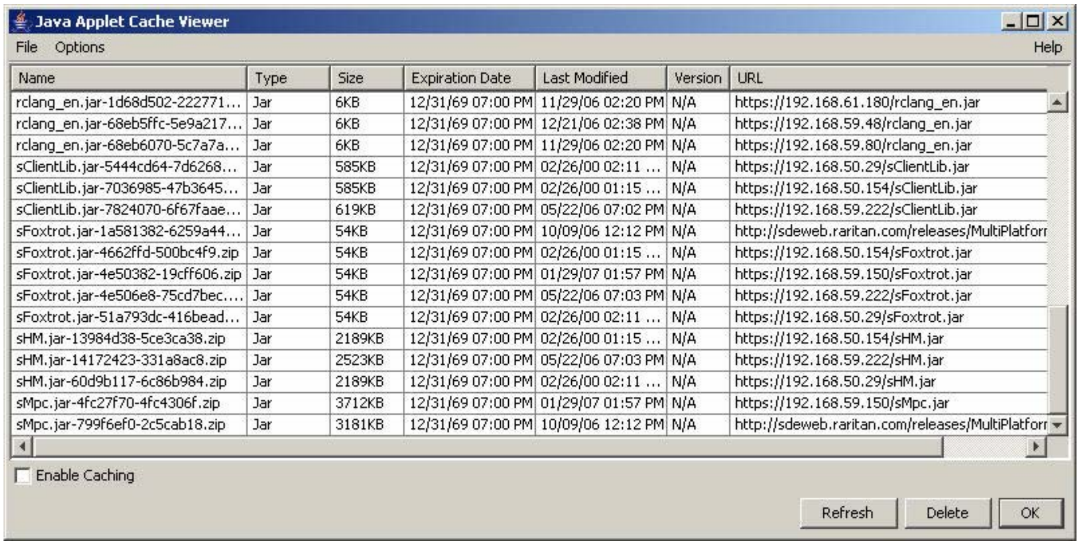
Settings

Location: ion Data\Sun\Java\Deployment\cache

Amount of disk space to use: ● Unlimited ○ Maximum MB

Jar compression: None

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



Java Applet Cache Viewer

Name	Type	Size	Expiration Date	Last Modified	Version	URL
rclang_en.jar-1d68d502-222771...	Jar	6KB	12/31/69 07:00 PM	11/29/06 02:20 PM	N/A	https://192.168.61.180/rclang_en.jar
rclang_en.jar-68eb5ffc-5e9a217...	Jar	6KB	12/31/69 07:00 PM	12/21/06 02:38 PM	N/A	https://192.168.59.48/rclang_en.jar
rclang_en.jar-68eb6070-5c7a7a...	Jar	6KB	12/31/69 07:00 PM	11/29/06 02:20 PM	N/A	https://192.168.59.80/rclang_en.jar
sClientLib.jar-5444cd64-7d6268...	Jar	585KB	12/31/69 07:00 PM	02/26/00 02:11 ...	N/A	https://192.168.50.29/sClientLib.jar
sClientLib.jar-7036985-47b3645...	Jar	585KB	12/31/69 07:00 PM	02/26/00 01:15 ...	N/A	https://192.168.50.154/sClientLib.jar
sClientLib.jar-7824070-6f67faae...	Jar	619KB	12/31/69 07:00 PM	05/22/06 07:02 PM	N/A	https://192.168.59.222/sClientLib.jar
sFoxtrot.jar-1a581382-6259a44...	Jar	54KB	12/31/69 07:00 PM	10/09/06 12:12 PM	N/A	http://sdeweb.raritan.com/releases/MultiPlatforr
sFoxtrot.jar-4662ffd-500bc4f9.zip	Jar	54KB	12/31/69 07:00 PM	02/26/00 01:15 ...	N/A	https://192.168.50.154/sFoxtrot.jar
sFoxtrot.jar-4e50382-19cff606.zip	Jar	54KB	12/31/69 07:00 PM	01/29/07 01:57 PM	N/A	https://192.168.59.150/sFoxtrot.jar
sFoxtrot.jar-4e506e8-75cd7bec....	Jar	54KB	12/31/69 07:00 PM	05/22/06 07:03 PM	N/A	https://192.168.59.222/sFoxtrot.jar
sFoxtrot.jar-51a793dc-416bead...	Jar	54KB	12/31/69 07:00 PM	02/26/00 02:11 ...	N/A	https://192.168.50.29/sFoxtrot.jar
sHM.jar-13984d38-5ce3ca38.zip	Jar	2189KB	12/31/69 07:00 PM	02/26/00 01:15 ...	N/A	https://192.168.50.154/sHM.jar
sHM.jar-14172423-331a8ac8.zip	Jar	2523KB	12/31/69 07:00 PM	05/22/06 07:03 PM	N/A	https://192.168.59.222/sHM.jar
sHM.jar-60d9b117-6c86b984.zip	Jar	2189KB	12/31/69 07:00 PM	02/26/00 02:11 ...	N/A	https://192.168.50.29/sHM.jar
sMpc.jar-4fc27f70-4fc4306f.zip	Jar	3712KB	12/31/69 07:00 PM	01/29/07 01:57 PM	N/A	https://192.168.59.150/sMpc.jar
sMpc.jar-799f6ef0-2c5cab18.zip	Jar	3181KB	12/31/69 07:00 PM	10/09/06 12:12 PM	N/A	http://sdeweb.raritan.com/releases/MultiPlatforr

□ Enable Caching

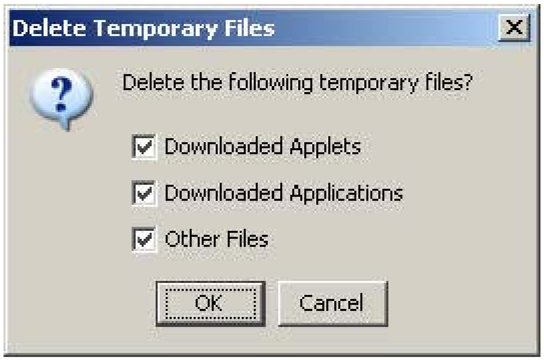
c. Deselect the Enable Caching checkbox if it is already checked.

d. Click OK.

4. To clear the Java cache:

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

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



5. Click OK.

➢ *To check the JRE version in Linux:*

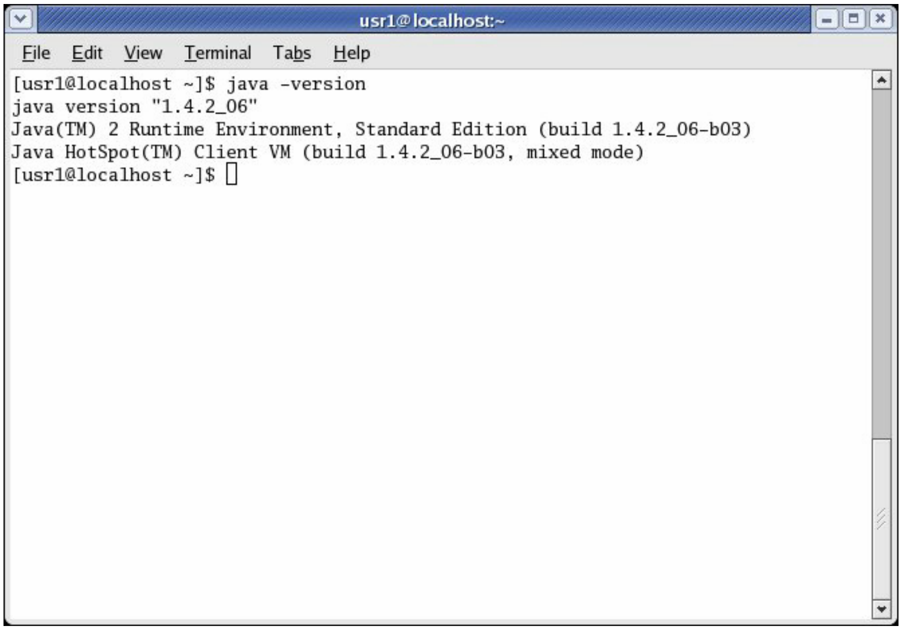
1. In a graphical environment, open a terminal dialog.
2. Type java version in the command line and press Enter on your keyboard. The currently-installed version of Java Runtime Environment (JRE) is displayed.

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

3. Set your path:
   a. To set your path and assuming JRE 1.4.2_05 is installed in /usr/local/java: you must set your PATH variable.
   b. To set the path for bash shell, export PATH=$PATH:/usr/local/java/j2re1.4.2_05/bin.
   c. To set the path for tcsh or csh, set PATH = ($PATH /usr/local/java/j2re1.4.2_05/bin).

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

Refer to your shell documentation if you encounter problems.



```
[usr1@localhost ~]$ java -version
java version "1.4.2_06"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2_06-b03)
Java HotSpot(TM) Client VM (build 1.4.2_06-b03, mixed mode)
[usr1@localhost ~]$ 
```

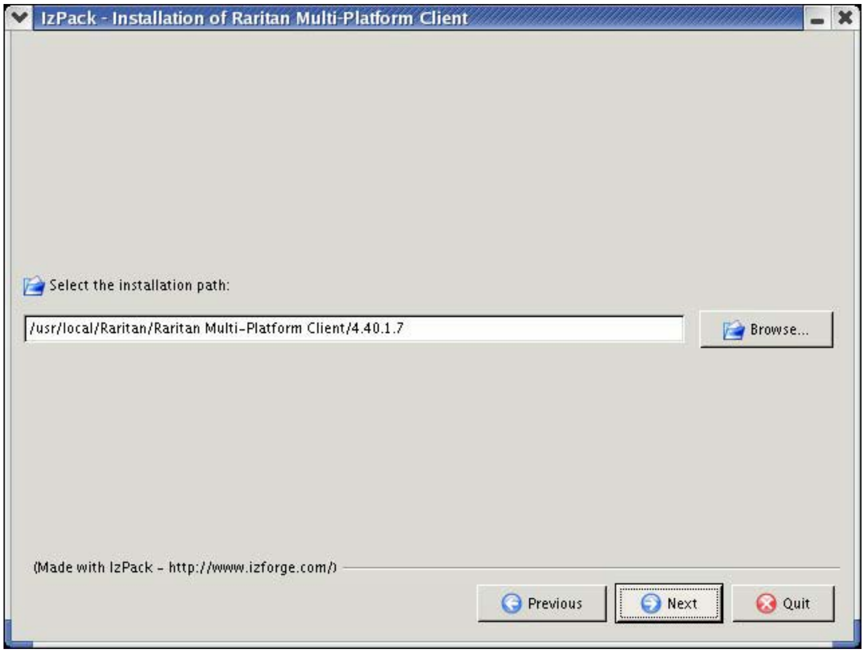
4. If the JRE is version 1.4.2_05 or higher, proceed with the MPC installation. If the version is prior to 1.4.2_05, go to the Java website at http://java.sun.com/products/ to download the latest Runtime Environment.

➢ *To install MPC for Linux:*

You must have Administrative privileges to install MPC.

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

4. After the initial page loads, click Next.



IzPack - Installation of Raritan Multi-Platform Client
Browse...
(Made with IzPack - http://www.izforge.com/)
Previous
Next
Quit

Select the installation path:

/usr/local/Raritan/Raritan Multi-Platform Client/4.40.1.7

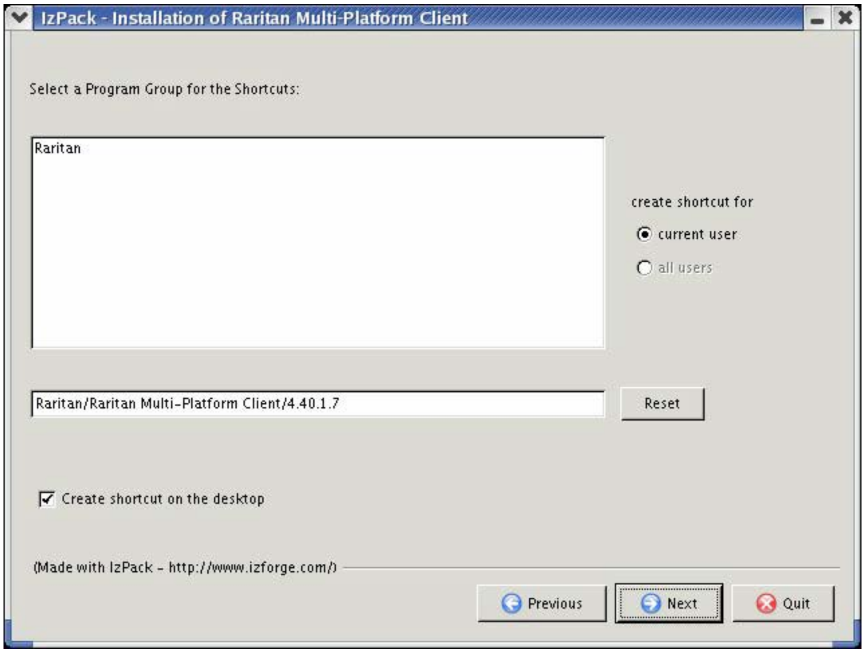
5. Use the Browse function to select a directory to install MPC if the directory is different from the default path displayed in the "Select the installation path" field.

6. Click Next to open the Shortcut dialog.

7. On the Shortcut dialog:

   - Choose a shortcut location from the "Select a Program Group for the Shortcuts:" field.
   - Select either "current user" or "all users" to define who should have access to the shortcut.
   - Check the "Create shortcut on the desktop" checkbox if you want the shortcut to appear on the desktop.

8. When finished, click Next.



IzPack - Installation of Raritan Multi-Platform Client

Select a Program Group for the Shortcuts:

Raritan

create shortcut for

● current user

○ all users

Raritan/Raritan Multi-Platform Client/4.40.1.7

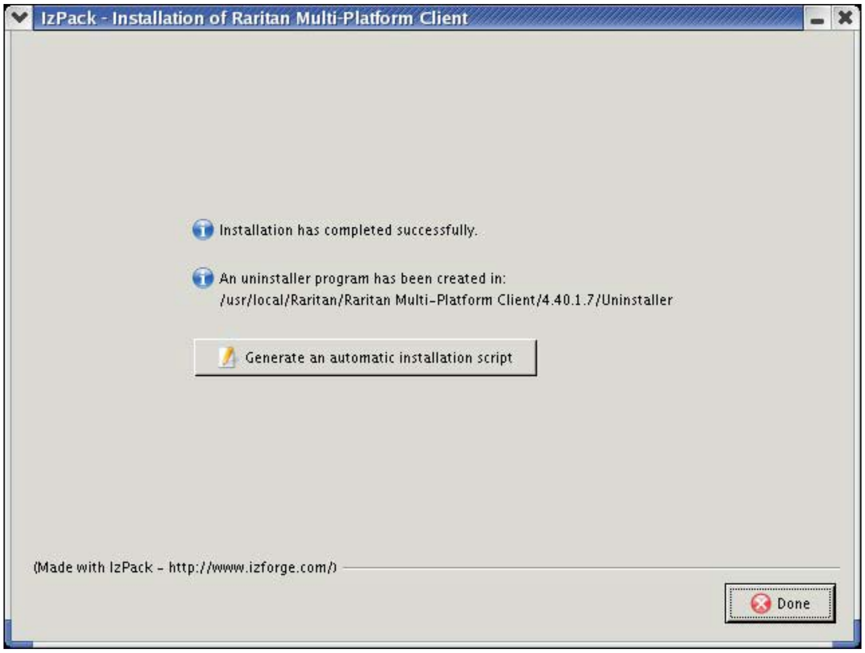
☑ Create shortcut on the desktop

(Made with IzPack - http://www.izforge.com/)

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

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

9. Click Done to close the Installation dialog.



IzPack - Installation of Raritan Multi-Platform Client

Installation has completed successfully.

An uninstaller program has been created in:
/usr/local/Raritan/Raritan Multi-Platform Client/4.40.1.7/Uninstaller

Generate an automatic installation script
(Made with IzPack - http://www.izforge.com/)
Done

➢ *To open MPC in Linux:*

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

Solaris

To check the JRE version for Sun Solaris:

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

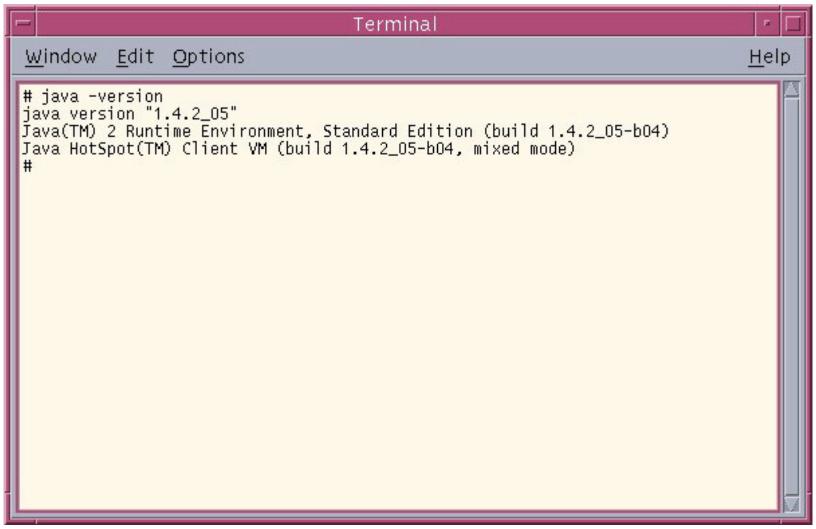
   If your path variable is not set to where the java binaries have been installed, you may not be able to see the JRE version.

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

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

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

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



```
# java -version
java version "1.4.2_05"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2_05-b04)
Java HotSpot(TM) Client VM (build 1.4.2_05-b04, mixed mode)
#
```

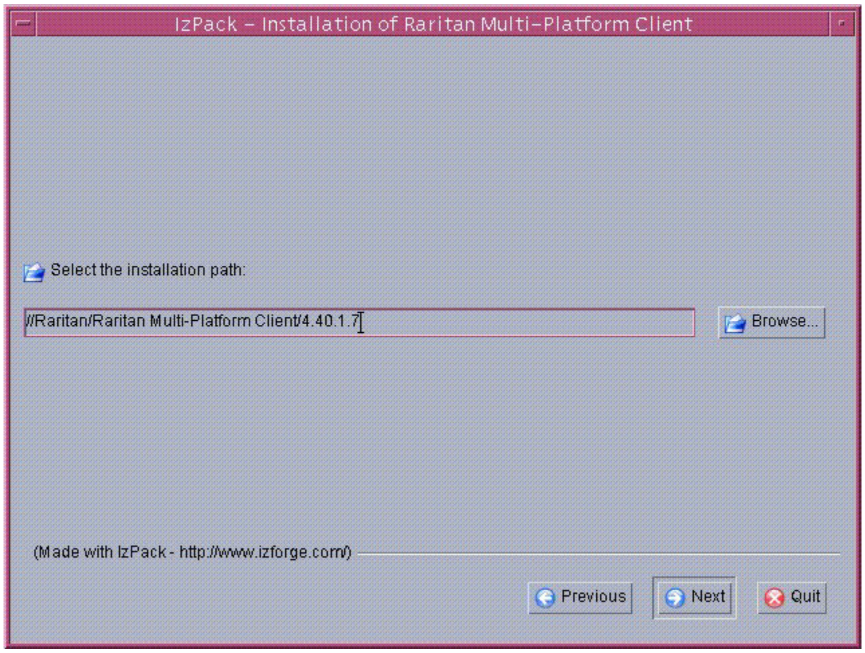
4. If the JRE is version 1.4.2_05 or higher, proceed with the MPC installation. If the version is prior to 1.4.2_05, go to the Sun website at http://java.sun.com/products/ to download the latest Runtime Environment.

➢ *To install MPC for Sun Solaris:*

You must have administrative privileges to install MPC.

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

4. After the initial page loads, click Next.



IzPack - Installation of Raritan Multi-Platform Client

Select the installation path:

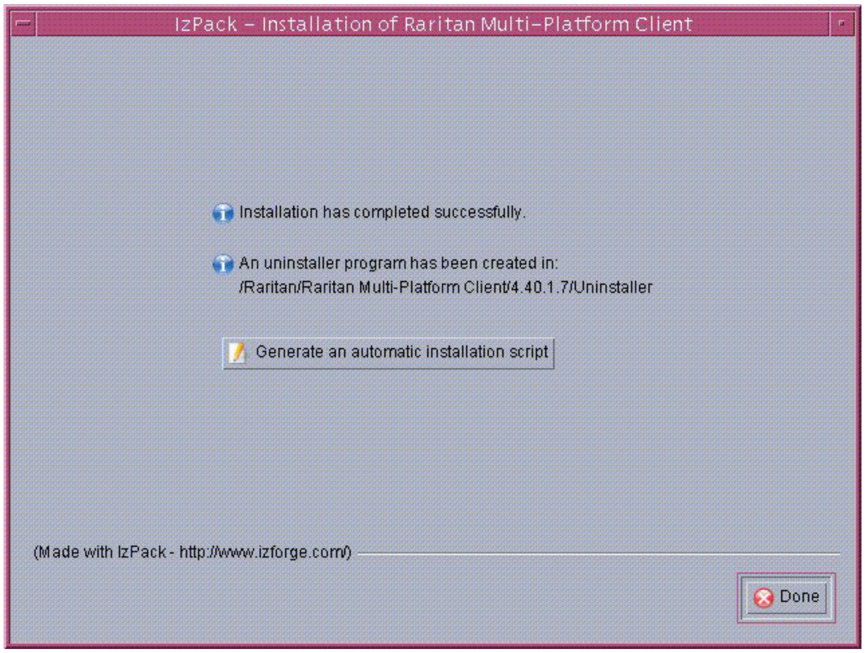
//Raritan/Raritan Multi-Platform Client/4.40.1.7

(Made with IzPack - http://www.izforge.com/)

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

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

9. Click Done to close the Installation dialog.



IzPack - Installation of Raritan Multi-Platform Client

Installation has completed successfully.

An uninstaller program has been created in:
/Raritan/Raritan Multi-Platform Client/4.40.1.7/Uninstaller

Generate an automatic installation script
(Made with IzPack - http://www.izforge.com/)
Done

➢ *To open MPC in Sun Solaris:*

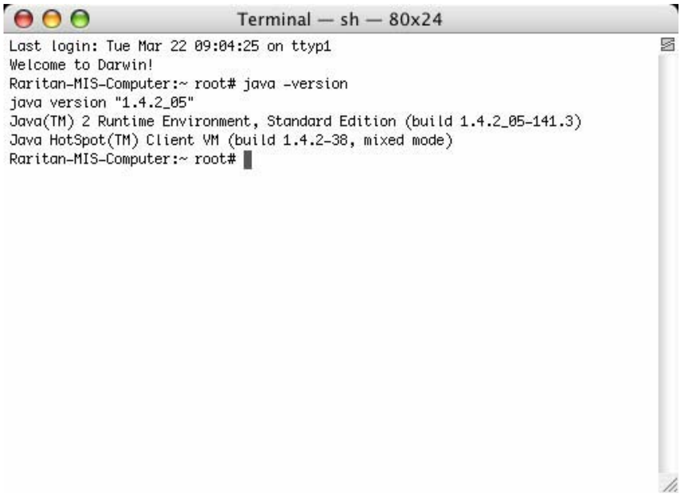
1. Open a terminal window and navigate to the directory where you installed MPC (the default location is /usr/local/Raritan/Raritan MPC/4.40.1.7).
2. Type *./start.sh* and press Enter to open MPC.
3. Double-click the desired device to establish a connection, type your user name and password, and click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

Macintosh

➢ *To check JRE on Macintosh:*

1. Launch a terminal window on the Macintosh desktop.

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



```
Last login: Tue Mar 22 09:04:25 on ttyp1
Welcome to Darwin!
Raritan-MIS-Computer:~ root# java -version
java version "1.4.2_05"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2_05-141.3)
Java HotSpot(TM) Client VM (build 1.4.2-38, mixed mode)
Raritan-MIS-Computer:~ root#
```

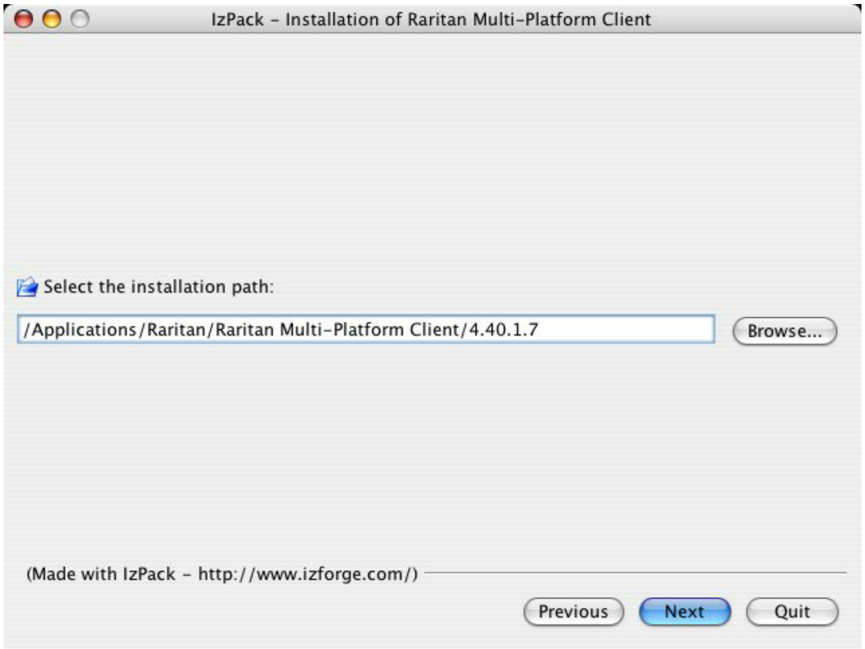
3. If the JRE is version 1.4.2_05 or higher, proceed with the MPC installation. If the version is prior to 1.4.2_05, go to the Apple website to download the latest Runtime Environment.

➢ *To install MPC on a Mac:*

You must have administrative privileges to install MPC.

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

4. After the initial dialog appears, click Next.



IzPack - Installation of Raritan Multi-Platform Client

Select the installation path:

/Applications/Raritan/Raritan Multi-Platform Client/4.40.1.7

(Made with IzPack - http://www.izforge.com/)

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

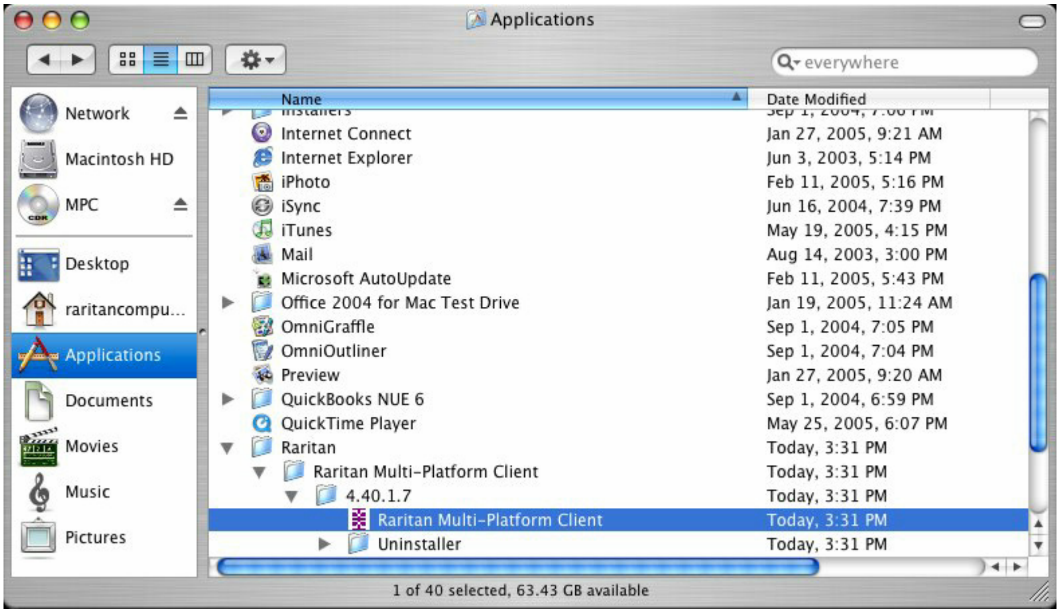
6. When installation is complete, click Next.

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

7. Click Done to close the Installation dialog.

➢ *To open MPC on a Mac:*

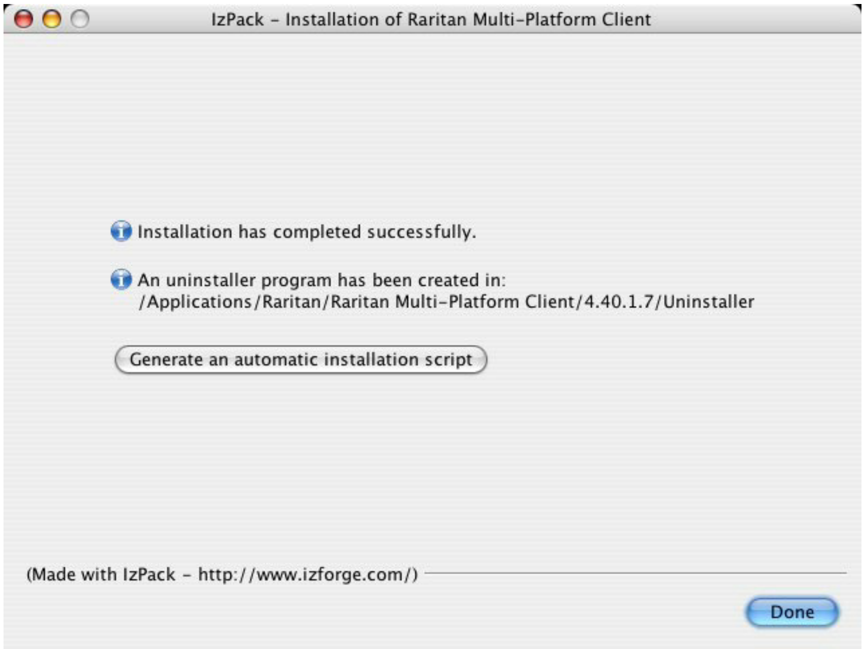
1. Open a Finder window and navigate to the directory where you installed MPC (the default location is /Applications/Raritan/Raritan MPC/4.40.1.7).



Name	Date Modified
Installers	Sep 1, 2004, 7:00 PM
Internet Connect	Jan 27, 2005, 9:21 AM
Internet Explorer	Jun 3, 2003, 5:14 PM
iPhoto	Feb 11, 2005, 5:16 PM
iSync	Jun 16, 2004, 7:39 PM
iTunes	May 19, 2005, 4:15 PM
Mail	Aug 14, 2003, 3:00 PM
Microsoft AutoUpdate	Feb 11, 2005, 5:43 PM
Office 2004 for Mac Test Drive	Jan 19, 2005, 11:24 AM
OmniGraffle	Sep 1, 2004, 7:05 PM
OmniOutliner	Sep 1, 2004, 7:04 PM
Preview	Jan 27, 2005, 9:20 AM
QuickBooks NUE 6	Sep 1, 2004, 6:59 PM
QuickTime Player	May 25, 2005, 6:07 PM
Raritan	Today, 3:31 PM
Raritan Multi-Platform Client	Today, 3:31 PM
4.40.1.7	Today, 3:31 PM
Raritan Multi-Platform Client	Today, 3:31 PM
Uninstaller	Today, 3:31 PM

1 of 40 selected, 63.43 GB available

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

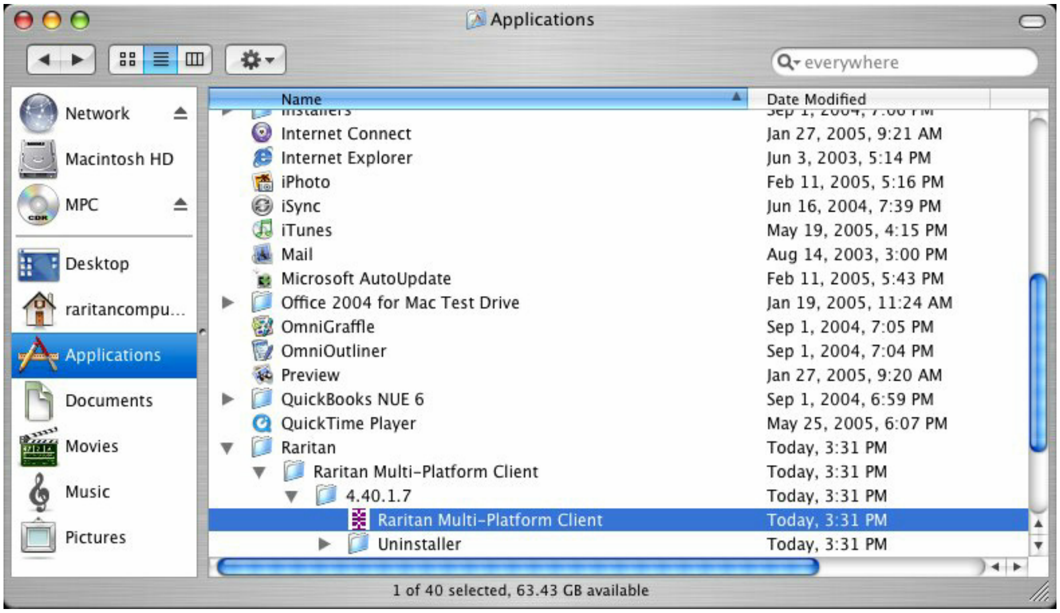

IzPack – Installation of Raritan Multi-Platform Client
Generate an automatic installation script
Done

Installation has completed successfully.

An uninstaller program has been created in:
/Applications/Raritan/Raritan Multi-Platform Client/4.40.1.7/Uninstaller

(Made with IzPack – http://www.izforge.com/)

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



Name	Date Modified
Installers	Sep 1, 2004, 7:00 PM
Internet Connect	Jan 27, 2005, 9:21 AM
Internet Explorer	Jun 3, 2003, 5:14 PM
iPhoto	Feb 11, 2005, 5:16 PM
iSync	Jun 16, 2004, 7:39 PM
iTunes	May 19, 2005, 4:15 PM
Mail	Aug 14, 2003, 3:00 PM
Microsoft AutoUpdate	Feb 11, 2005, 5:43 PM
Office 2004 for Mac Test Drive	Jan 19, 2005, 11:24 AM
OmniGraffle	Sep 1, 2004, 7:05 PM
OmniOutliner	Sep 1, 2004, 7:04 PM
Preview	Jan 27, 2005, 9:20 AM
QuickBooks NUE 6	Sep 1, 2004, 6:59 PM
QuickTime Player	May 25, 2005, 6:07 PM
Raritan	Today, 3:31 PM
Raritan Multi-Platform Client	Today, 3:31 PM
4.40.1.7	Today, 3:31 PM
Raritan Multi-Platform Client	Today, 3:31 PM
Uninstaller	Today, 3:31 PM

1 of 40 selected, 63.43 GB available

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

Modem Connectivity in MPC

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

1. As the root, change the group for /etc/ppp directory and required files:

   a. chgrp uucp /etc/ppp

   b. chgrp uucp /etc/ppp/pap-secrets

   c. chgrp uucp /etc/ppp/peers

2. Change the permissions for /etc/ppp chmod g+rwx /etc/ppp

3. Change the permissions for /etc/ppp/pap-secrets chmod g+rwx /etc/ppp/pap-secrets

4. Change the permissions for /etc/ppp/peers chmod g+rwx /etc/ppp/peers

5. Set the suid bit to pppd chmod u+s /usr/sbin/pppd (/usr/bin/pppd depending on the location of pppd)

6. Assign users to the uucp group:
   a. /usr/sbin/usermod -G {existing groups for user1},uucp user1
   b. /usr/sbin/usermod -G {existing groups for user2},uucp user2, and so forth.
7. When logged on as the normal user, update the path for access to pppd and the chat export PATH=$PATH:/usr/sbin (/usr/bin depending on the location of pppd).

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

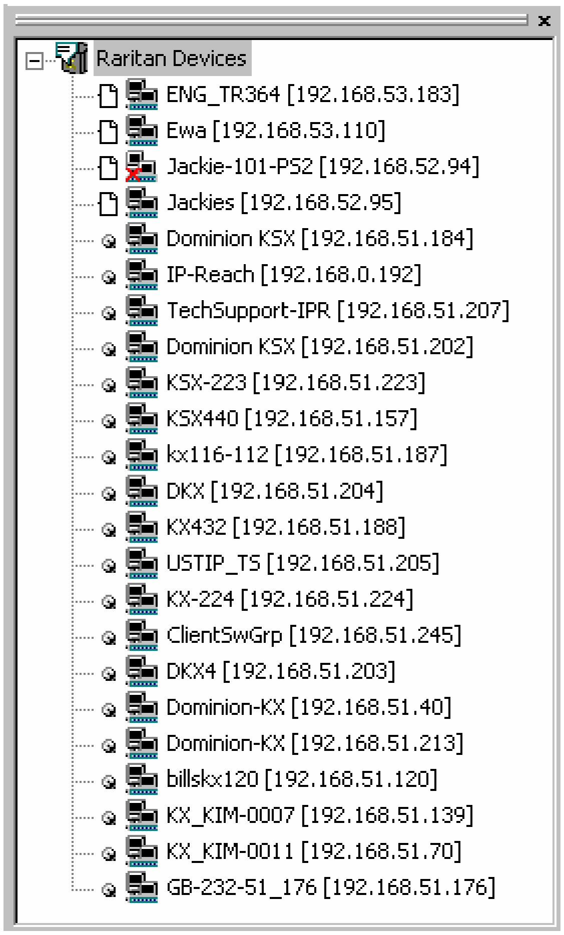
Operation

Window Layout

Navigator

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

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



Raritan Devices

- ENG_TR364 [192.168.53.183]
- Ewa [192.168.53.110]
- Jackie-101-PS2 [192.168.52.94]
- Jackies [192.168.52.95]
- Dominion KSX [192.168.51.184]
- IP-Reach [192.168.0.192]
- TechSupport-IPR [192.168.51.207]
- Dominion KSX [192.168.51.202]
- KSX-223 [192.168.51.223]
- KSX440 [192.168.51.157]
- kx116-112 [192.168.51.187]
- DKX [192.168.51.204]
- KX432 [192.168.51.188]
- USTIP_TS [192.168.51.205]
- KX-224 [192.168.51.224]
- ClientSwGrp [192.168.51.245]
- DKX4 [192.168.51.203]
- Dominion-KX [192.168.51.40]
- Dominion-KX [192.168.51.213]
- billskx120 [192.168.51.120]
- KX_KIM-0007 [192.168.51.139]
- KX_KIM-0011 [192.168.51.70]
- GB-232-51_176 [192.168.51.176]

Devices in the MPC Navigator

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

Device Ports in the Navigator

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

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

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

Navigator Icons

Each device in the Navigator is assigned two icons. One icon represents the device's connection profile and the other icon represents its network status. A connection profile is generally created by a user in order to store personalized information about specific devices (see ***Creating Profiles*** (on page 127) for additional information). The connection status indicates the current status of the device.

Device Connection Profile Icons (Left Icon)

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

Device Network Status Icons (Right Icon)

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

Port Connection Status Icons

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

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

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

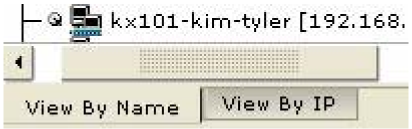
Customizing the Navigator

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

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

MPC Navigator Tabs

MPC tabs at the base of its Navigator pane. These tabs allow you to change how you display devices. Click the View By Name tab to sort the list alphabetically by name or click the View By IP tab to sort the list numerically by IP address.



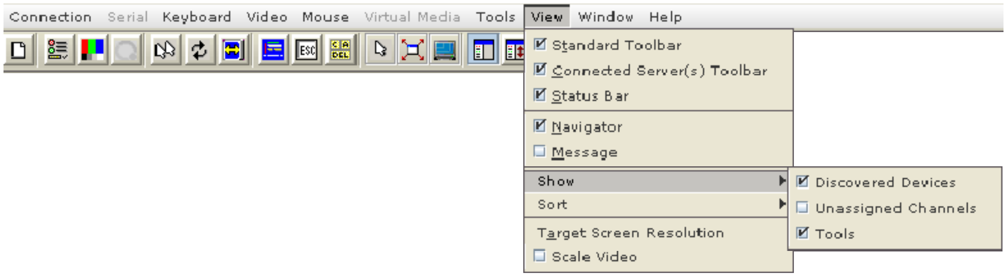
Note that these tabs are available only in the MPC interface.

Navigator Display and Sort Options

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

Showing Ports

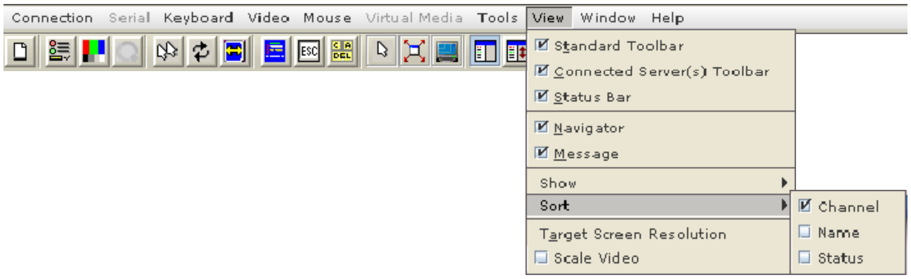
- Discovered Devices - Shows or hides discovered devices from the Navigator view. You will not see broadcast messages when this option is disabled (not selected).
- Unassigned Channels - Shows or hides channels with no assigned targets. Note that the default for Generation 1 (G1) devices is to show unassigned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



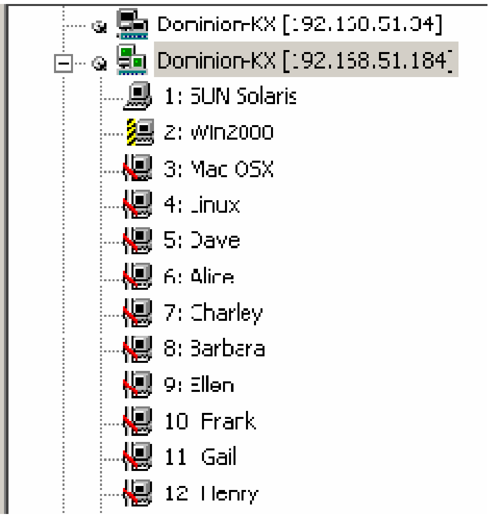
Note: These settings are saved from session to session.

Sorting Ports

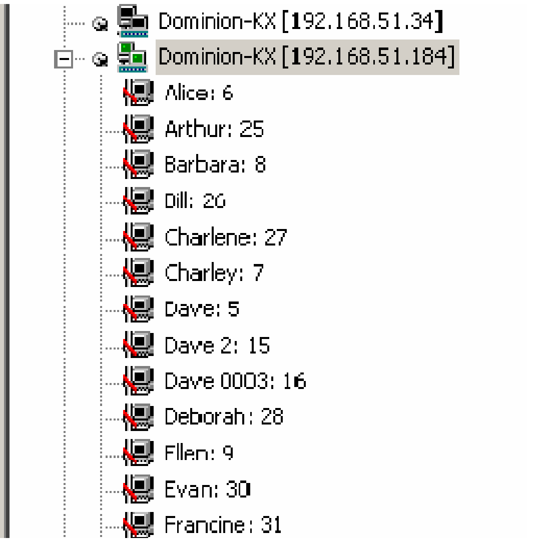
Use the Sort options on the View menu to organize port information. You are able to sort ports by channel number, channel name, or channel status.



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



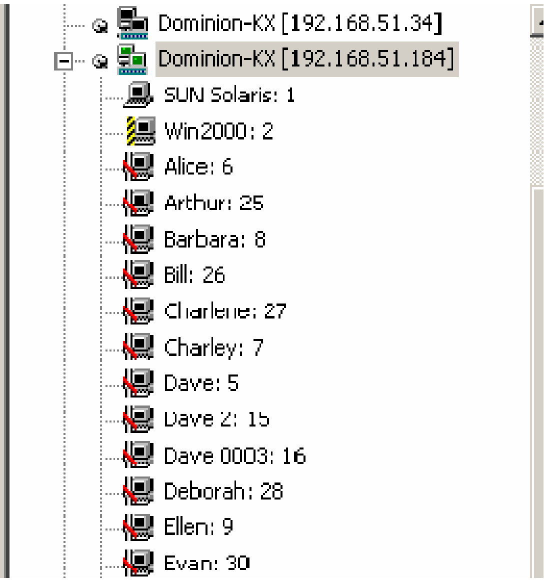
Name - When sorted by name (View > Sort > Name), port names are sorted alphanumerically within each group.



Dominion-KX [192.168.51.34]
Dominion-KX [192.168.51.184]
Alice: 6
Arthur: 25
Barbara: 8
Dill: 26
Charlene: 27
Charley: 7
Dave: 5
Dave 2: 15
Dave 0003: 16
Deborah: 28
Fllen: 9
Evan: 30
Francine: 31

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

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



Dominion-KX [192.168.51.34]
Dominion-KX [192.168.51.184]
SUN Solaris: 1
Win2000: 2
Alice: 6
Arthur: 25
Barbara: 8
Bill: 26
Charlene: 27
Charley: 7
Dave: 5
Dave 2: 15
Dave 0003: 16
Deborah: 28
Ellen: 9
Evan: 30

Toolbars

Standard Toolbar

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

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

- Choose View > Standard Toolbar.

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

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

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

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

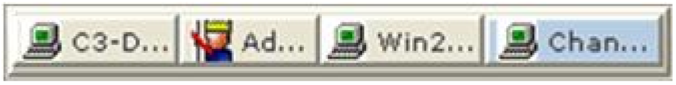
MPC Connected Server(s) Toolbar

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

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

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

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



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

- Choose View > Connected Server(s) Toolbar.

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

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

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

Status Bar

The status bar displays session information about your connection to a Raritan device. This information includes:

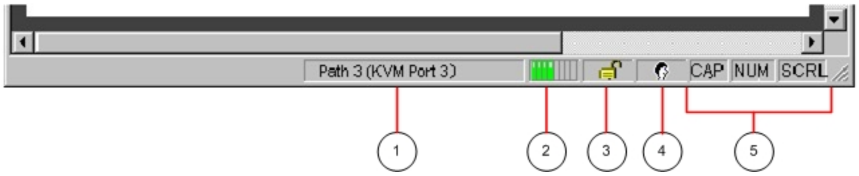


Diagram key	Session information	Description
①	Video sensing status/path indicator	Indicates when video sensing occurs during connections to target KVM server ports.
②	Bandwidth usage indicator	Indicates how much of your total available bandwidth is currently being used. The connection speed setting determines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

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

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

Screen Modes

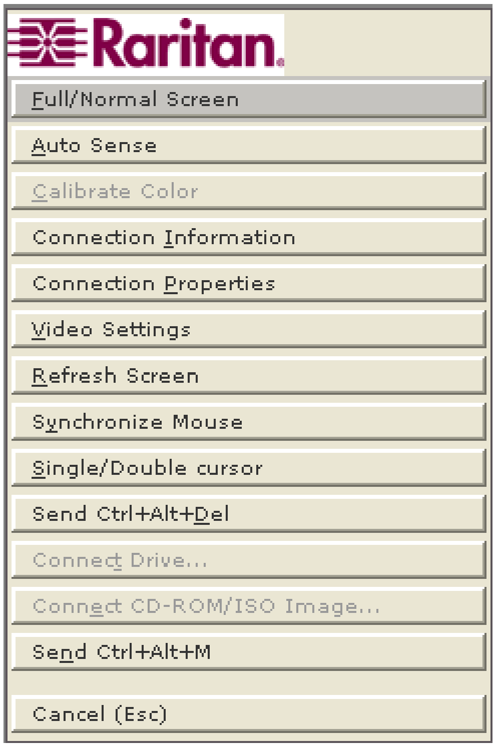
Besides a standard view, full screen view and a scaling option are available. These options increase the remote desktop area and make viewing the target video easier.

MPC Target Screen Resolution Mode

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

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

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



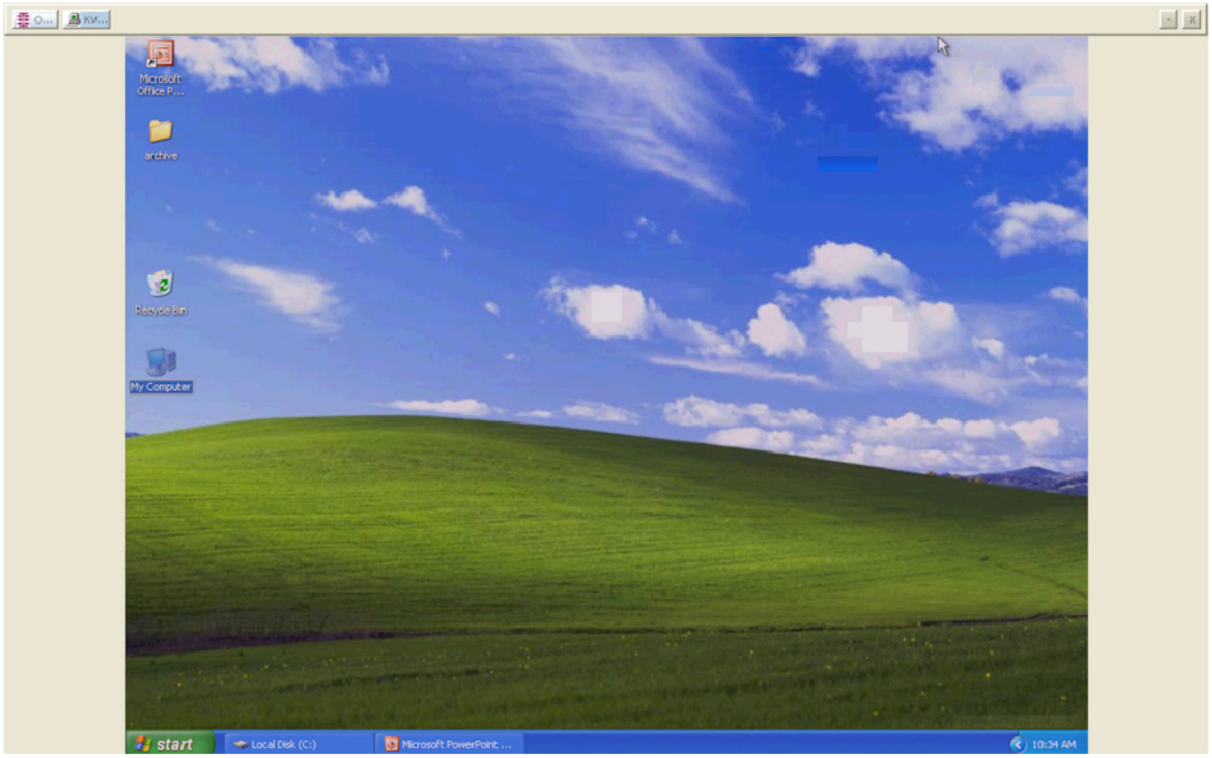
To exit full screen mode, use the shortcut menu or click the Close icon ☒ that appears at the top right of the page when you hover your mouse along the top of the screen.

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

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

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

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

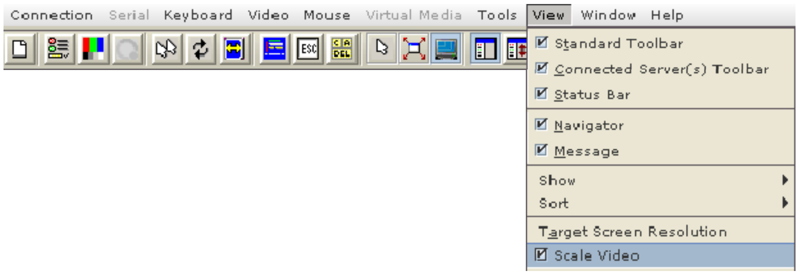


MPC Scaling

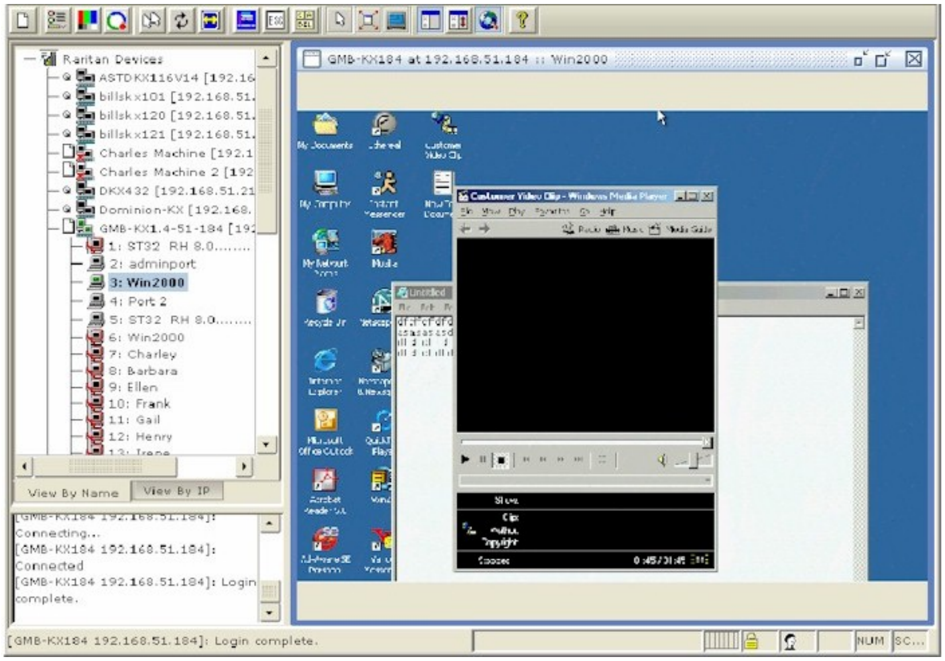
Scaling your target window size allows you to view the entire contents of the target server window. This feature increases or reduces the size of the target video to fit the window size and maintains the aspect ratio. This allows you to see the entire target server desktop while in standard view.

➢ ***To activate Scaling, do one of the following:***

- Choose View > Scale Video.



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



```
[GMB-KX184 192.168.51.184]:
Connecting...
[GMB-KX184 192.168.51.184]:
Connected
[GMB-KX184 192.168.51.184]: Login
complete.
```

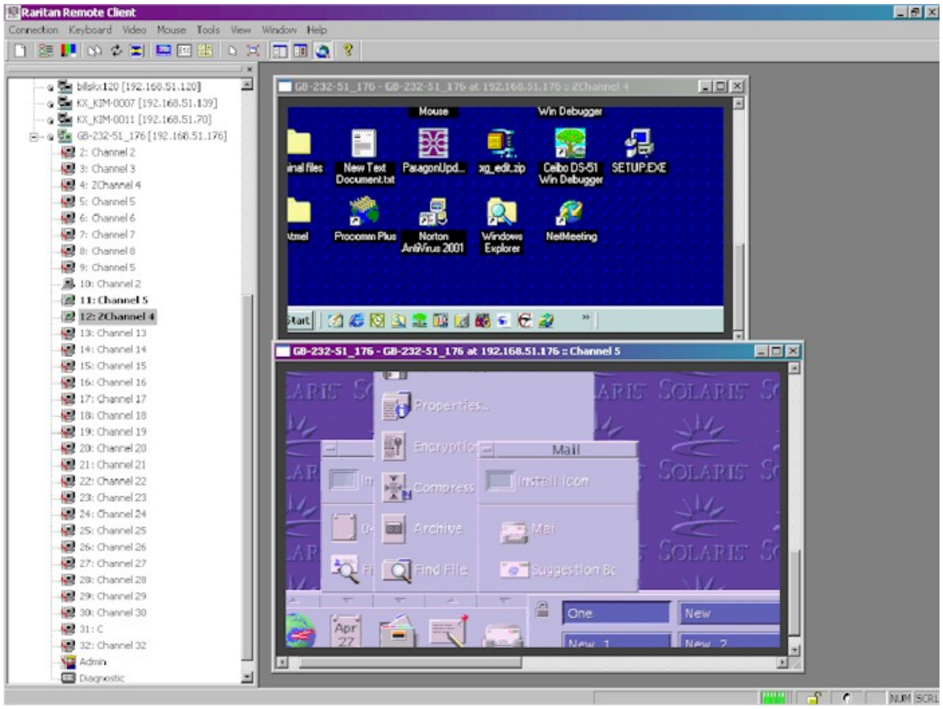
[GMB-KX184 192.168.51.184]: Login complete.

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

Auto-Scroll

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

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



Connection Profiles

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

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

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

Creating Profiles

➢ ***To create a profile:***

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

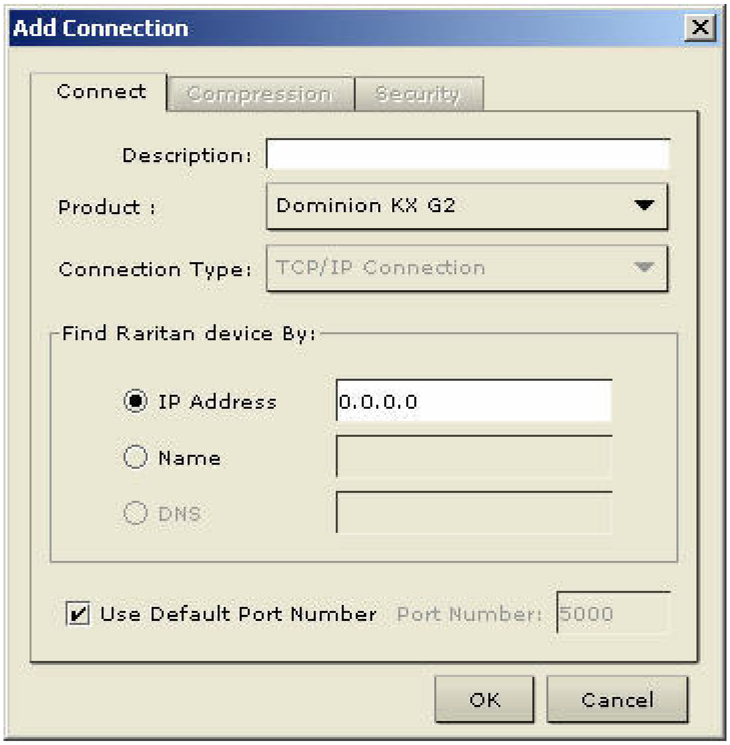
   The Add Connection dialog appears. Options are organized into three tabs.
2. On the Connect tab, type a meaningful description of the device in the Description field (up to 32 alphanumeric, special characters are allowed). This description identifies the Raritan device in the Navigator.
3. From the Product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

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

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

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

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


Add Connection

Description:

Product : Dominion KX G2

Connection Type: TCP/IP Connection

Find Raritan device By:

● IP Address 0.0.0.0

○ Name

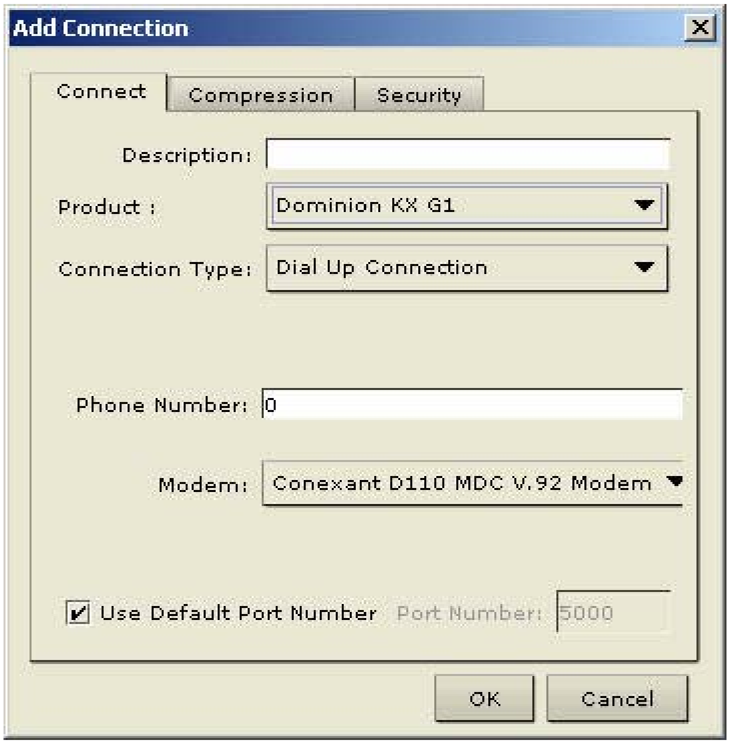
○ DNS

☑ Use Default Port Number Port Number: 5000

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

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

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



Add Connection

Description:

Product : Dominion KX G1

Connection Type: Dial Up Connection

Phone Number: 0

Modem: Conexant D110 MDC V.92 Modem

☑ Use Default Port Number Port Number: 5000

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

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

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

   - Auto Detect
   - 100mb Ethernet
   - 10mb Ethernet
   - 1.5mb (Max DSL/T1)
   - 1mb (Fast DSL/T1)
   - 512 kb (Medium DSL/T1)
   - 384 kb (Slow DSL/T1)

- 256 kb (Cable)
- 128 kb (Dual ISDN)
- 56 kb (ISP Modem)
- 33 kb (Fast Modem)
- 24 kb (Slow Modem)

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

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

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

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

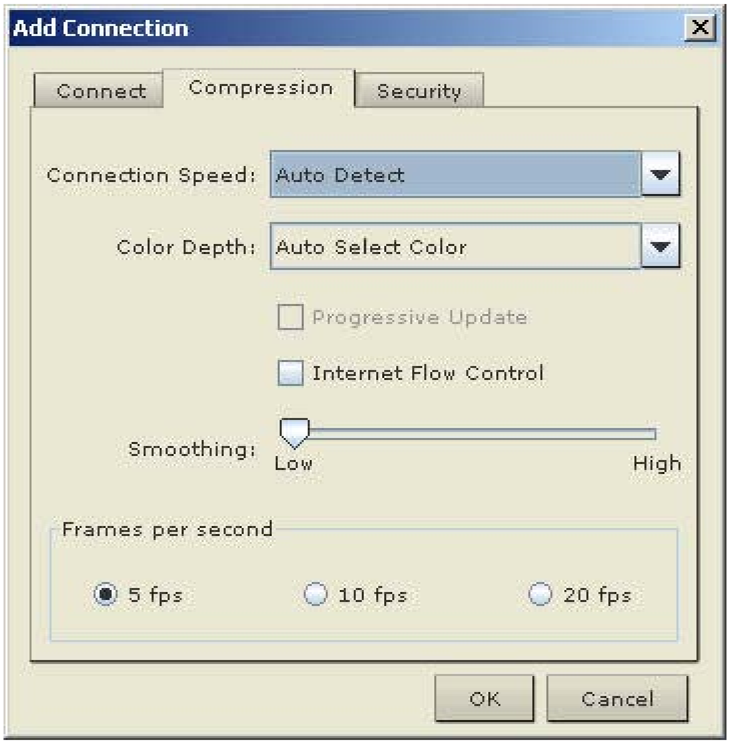
Note: When Color Depth is set to Auto Select Color (default), Progressive Update is automatic. The device will enable/disable Progressive Update as required, disabling it for fast connections and enabling it for slow connections.

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

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

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

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



Add Connection

Connection Speed: Auto Detect

Color Depth: Auto Select Color

□ Progressive Update

□ Internet Flow Control

Smoothing: Low — High

Frames per second

● 5 fps ○ 10 fps ○ 20 fps

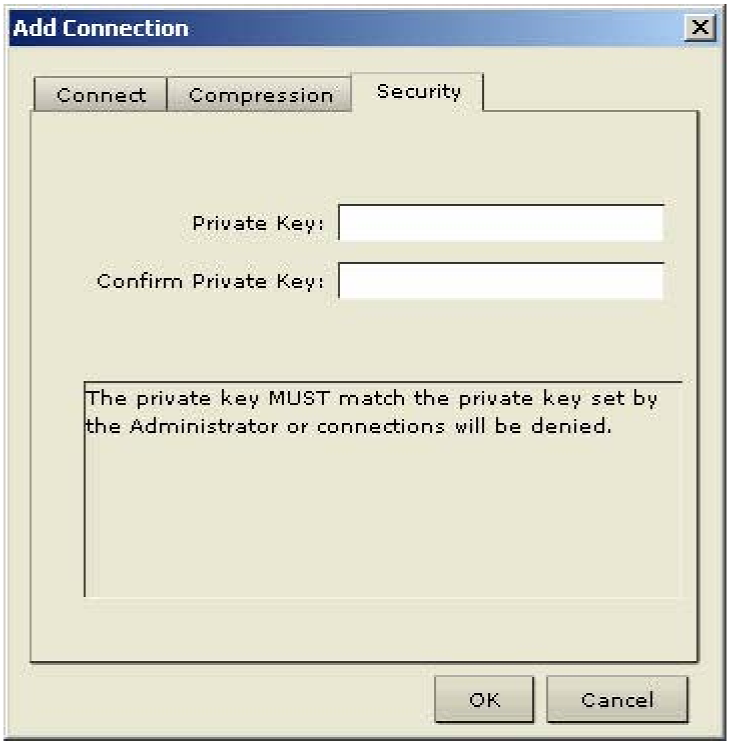
2. Update the Security tab.

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

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

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

3. Click OK to create the connection profile.



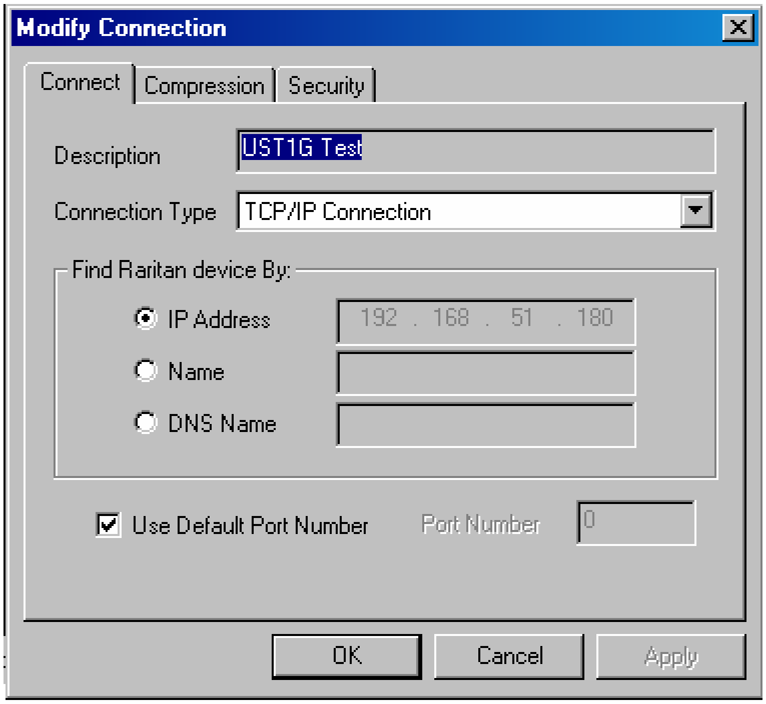
The private key MUST match the private key set by the Administrator or connections will be denied.

Modifying Profiles

➢ ***To modify a profile:***

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

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



Description: UST1G Test

Connection Type: TCP/IP Connection

Find Raritan device By:

● IP Address 192 . 168 . 51 . 180

○ Name

○ DNS Name

☑ Use Default Port Number   Port Number 0

3. Update the fields as appropriate.

4. Click OK.

Deleting Profiles

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

1. Select the device with a profile in the Navigator and right-click it.

2. Choose Delete Profile.

3. When prompted to confirm the deletion, click Yes to delete the profile for this device or click No to return to the application without deleting.

Establishing a New Connection

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

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

Note: The default device login user name is admin and the default password is raritan. You have administrative privileges using these login credentials.

If you do not see an icon for your device in the Navigator, follow the instructions in ***Creating Profiles*** (on page 127) to create a new connection profile.

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

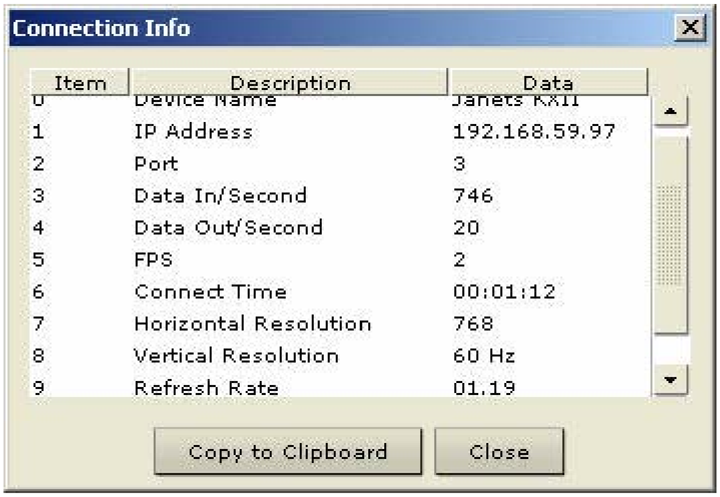
- User name - Raritan usernames *are not* case-sensitive.
- Password - Raritan passwords *are* case-sensitive.
- TCP Port - If you have configured your device to use a non-default TCP Port, this information must be entered into its connection profile.
- Firewall Settings - If you are accessing a device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

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

MPC Connection Information

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

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



Connection Info

Item	Description	Data
0	Device Name	Janets KXII
1	IP Address	192.168.59.97
2	Port	3
3	Data In/Second	746
4	Data Out/Second	20
5	FPS	2
6	Connect Time	00:01:12
7	Horizontal Resolution	768
8	Vertical Resolution	60 Hz
9	Refresh Rate	01.19

The following information is displayed about the current connection:

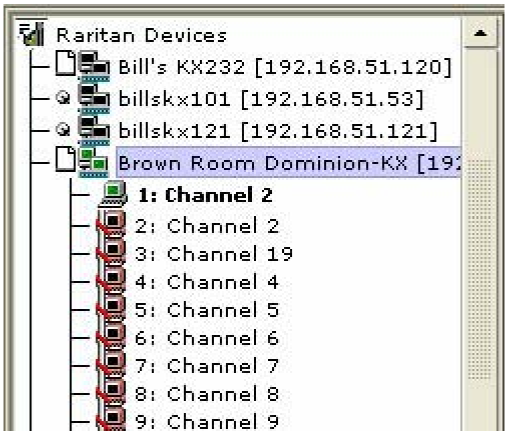
Connection information	Description
Device name	The name of your Dominion or IP-Reach device.
IP address	The IP Address of your Dominion or IP-Reach device.
Port	The KVM Communication TCP/IP Port used to access the target device.
Data in/second	Data rate in.
Data out/second	Data rate out.
FPS	The frames per second transmitted for video.
Connect time	The duration of the connect time.
Horizontal resolution	The page resolution horizontally.
Vertical resolution	The page resolution vertically.
Refresh rate	How often the page is refreshed.
Protocol version	The RFB Protocol version.

➢ ***To copy this information:***

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

Connect to a Remote KVM Console

Once you establish a connection with a Raritan device, that device's icon in the Navigator can be expanded to display all ports enabled for remote access.



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

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

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

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

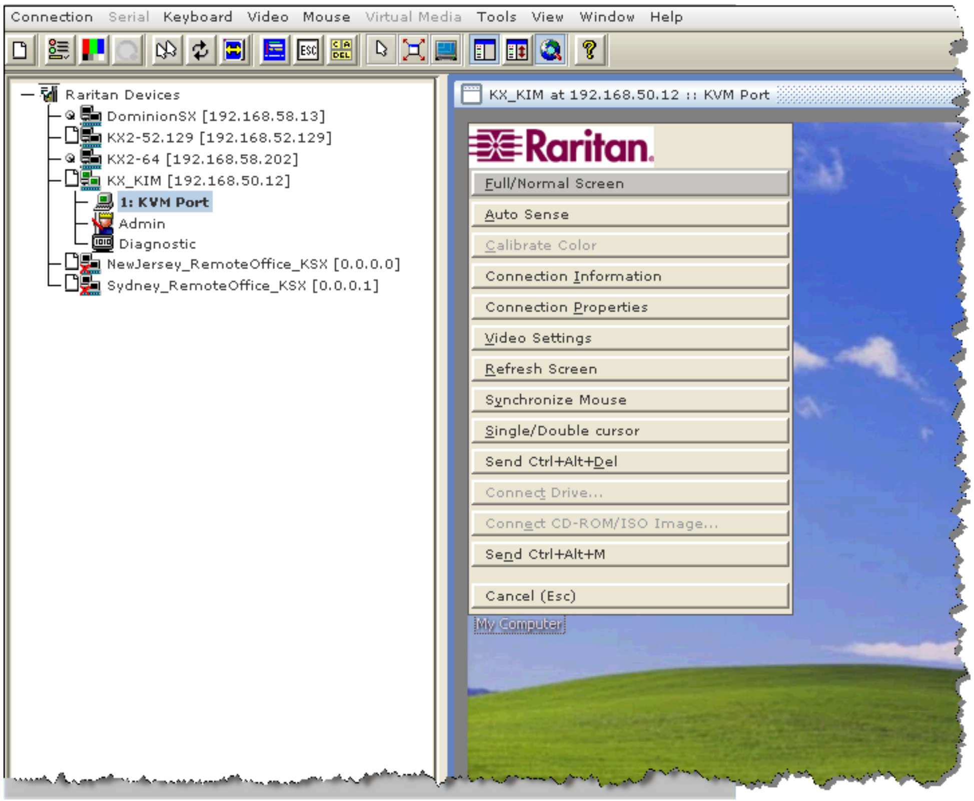
Shortcut Menu

To access the shortcut menu, use either the default keyboard combination of Ctrl+Left Alt+M or the keyboard combination you assign. See ***Changing the Shortcut Menu Keyboard Combination*** (on page 139) for more information.

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

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

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

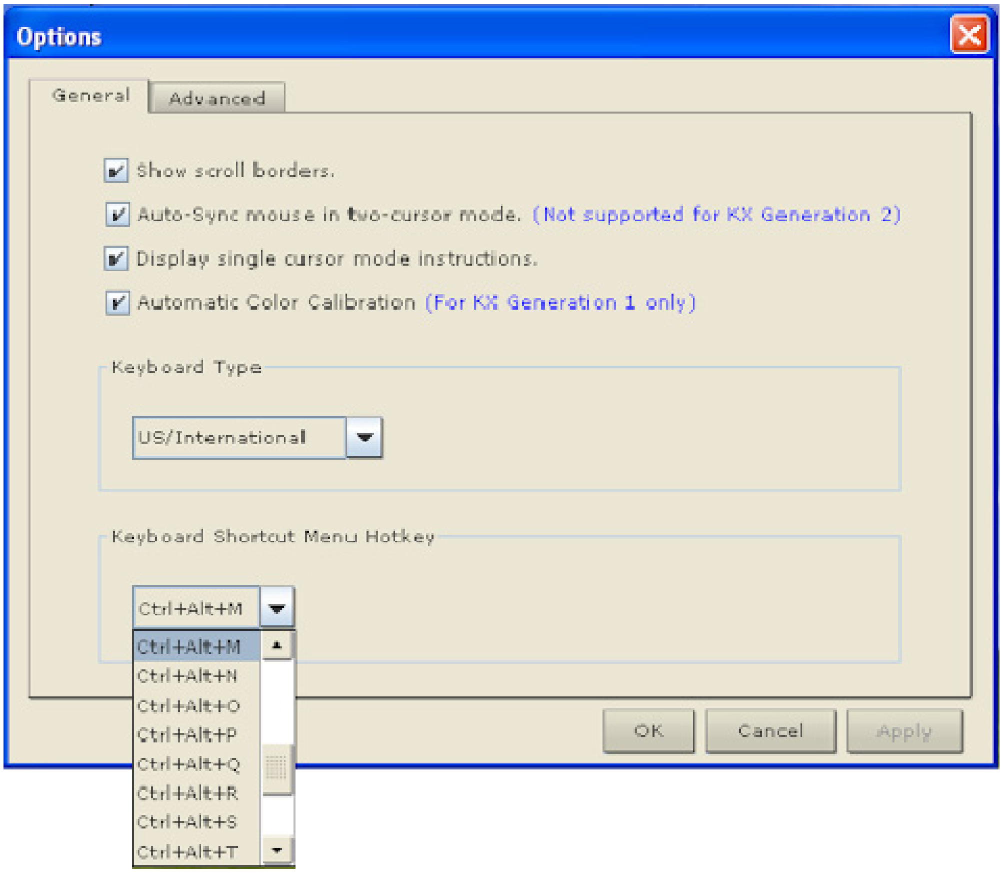


Changing the Shortcut Menu Keyboard Combination

➢ ***To change the keyboard combination, do the following:***

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

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



Options

General | Advanced

☑ Show scroll borders.

☑ Auto-Sync mouse in two-cursor mode. (Not supported for KX Generation 2)

☑ Display single cursor mode instructions.

☑ Automatic Color Calibration (For KX Generation 1 only)

Keyboard Type: US/International

Keyboard Shortcut Menu Hotkey: Ctrl+Alt+M

Ctrl+Alt+M
Ctrl+Alt+N
Ctrl+Alt+O
Ctrl+Alt+P
Ctrl+Alt+Q
Ctrl+Alt+R
Ctrl+Alt+S
Ctrl+Alt+T

Keyboard Macros

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

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

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

Building a Keyboard Macro

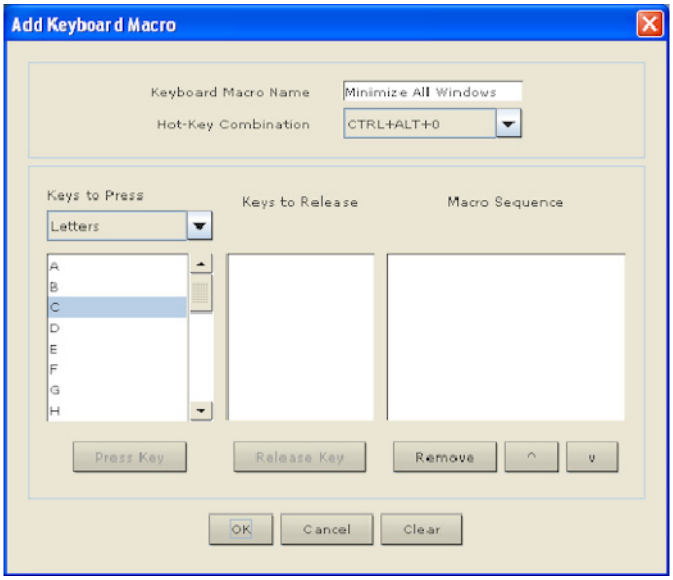
- ***To build a macro:***

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

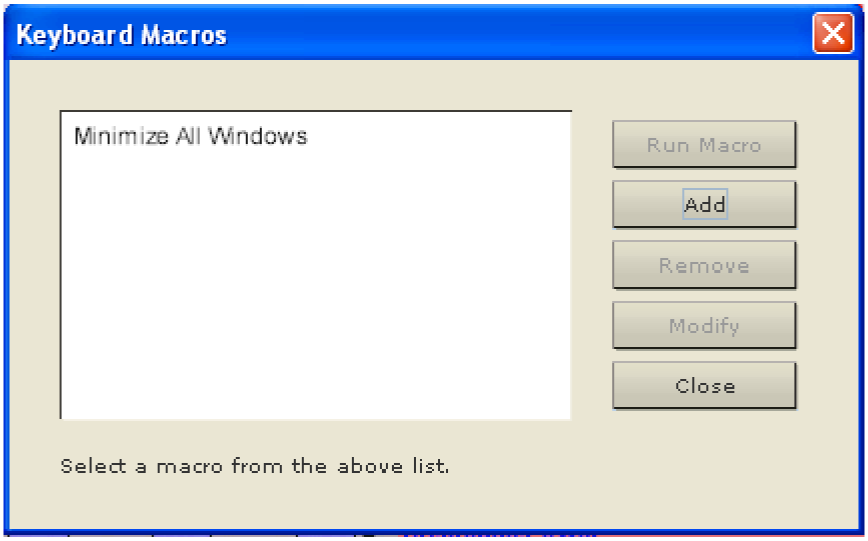
   As each key is selected, it will appear in the Keys to Release field. For example, select the Windows key and the letter D key. When these keys are selected in the client, the macro will be executed. Add a key release attribute to the macro if needed (see next step).

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

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



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



Select a macro from the above list.

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

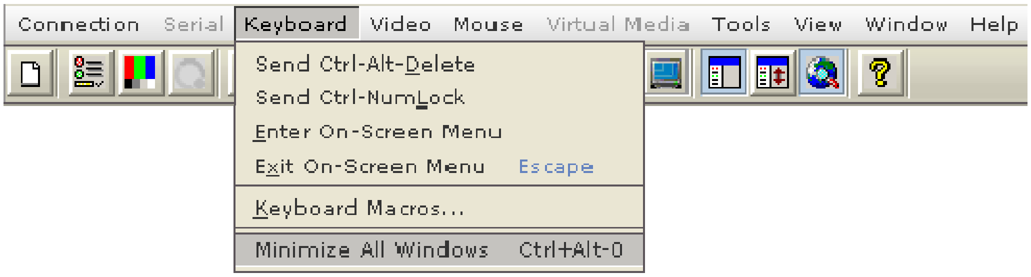
Note: Foreign keyboard layouts are not supported when using keyboard macros, except for those keys listed in the "Add Keyboard Macro" dialog for Japanese and Korean.

Running a Keyboard Macro

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

Run a Macro from the Menu Bar

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



Run a Macro Using a Keyboard Combination

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

Ctrl+Alt+Del Macro

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

In contrast, if you were to physically press the Ctrl+Alt+Del keys, the command would first be intercepted by your own PC due to the structure of the Windows operating system, instead of sending the key sequence to the target server as intended.

Common Hot Key Exceptions for MPC

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

Hot Key Combination	Description
Ctrl+Alt+Delete	Reboots the computer. The sequence is sent to the local system and the Windows Security (Task Manager, Shutdown, and so on) dialog is displayed.
Ctrl+Left Alt+M	Brings up the ***shortcut menu*** (on page 138).
Print Scrn	Treated locally and copies the page to the clipboard.

Following are limitations to specific keyboards and hot key combinations:

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

Windows Key in MPC

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

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

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

Keyboard Type

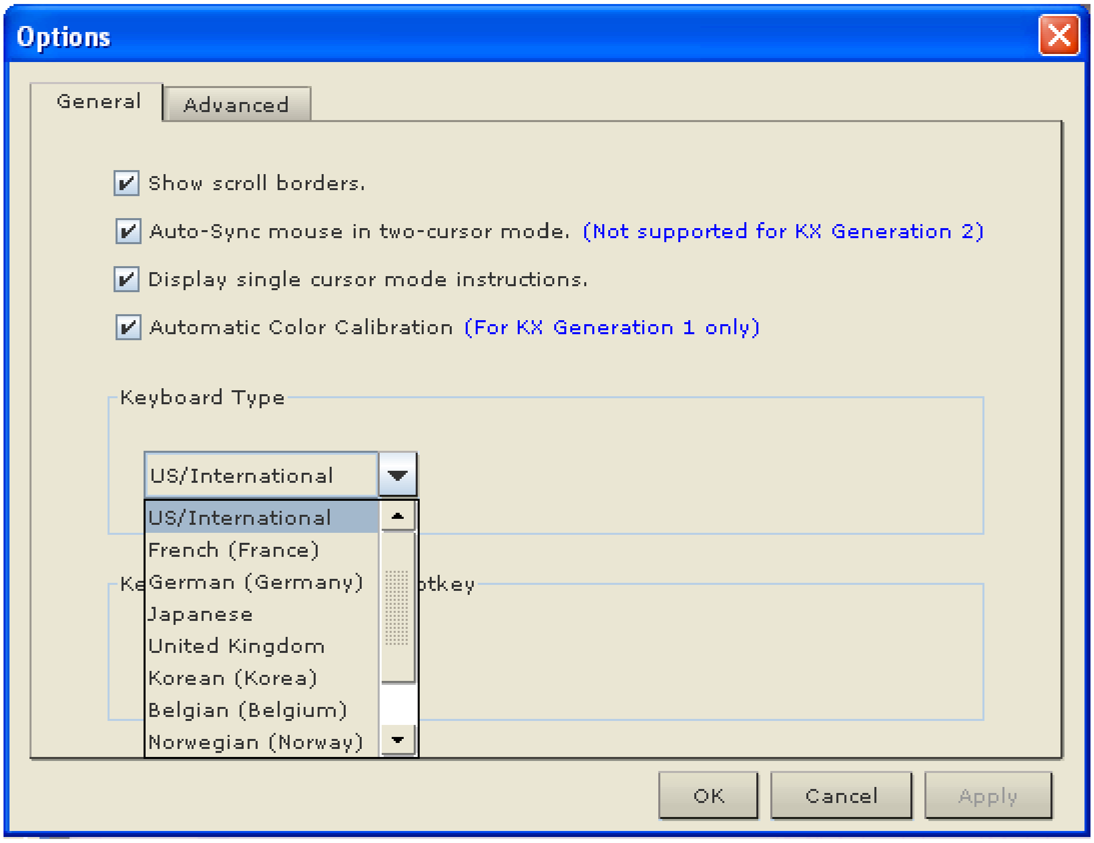
Specifying a Keyboard Type in MPC

MPC will not autodetect the type of keyboard you use, so you must specify your keyboard type to ensure accurate keyboard mapping.

➢ ***To specify a keyboard type:***

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

3. Click OK.



Options

General | Advanced

☑ Show scroll borders.

☑ Auto-Sync mouse in two-cursor mode. (Not supported for KX Generation 2)

☑ Display single cursor mode instructions.

☑ Automatic Color Calibration (For KX Generation 1 only)

Keyboard Type: US/International

Keyboard Limitations

Japanese Kanji Keyboards

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

Language Configuration on Linux

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

Language	Configuration method
US Intl	Default
UK	System Settings (Control Center)
French	Keyboard Indicator

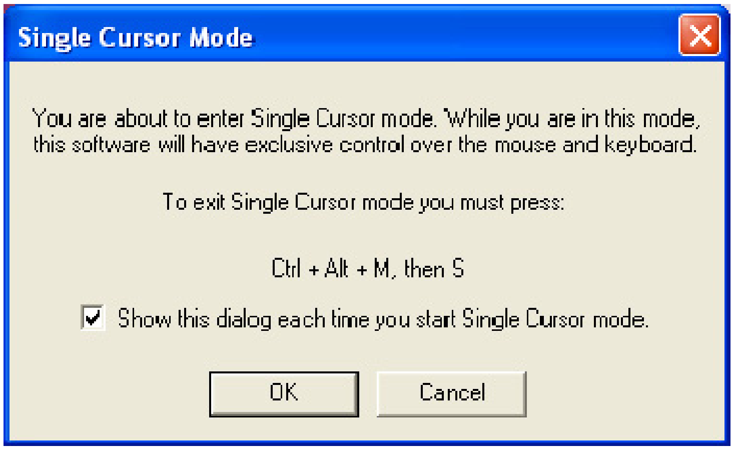
Language	Configuration method
German	System Settings (Control Center)
Norwegian	Keyboard Indicator
Swedish	Keyboard Indicator
Danish	Keyboard Indicator
Japanese	System Settings (Control Center)
Korean	System Settings (Control Center)
Hungarian	System Settings (Control Center)

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

Single Mouse Mode/Dual Mouse Mode

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

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



Single Cursor Mode

You are about to enter Single Cursor mode. While you are in this mode, this software will have exclusive control over the mouse and keyboard.

To exit Single Cursor mode you must press:

Ctrl + Alt + M, then S

☑ Show this dialog each time you start Single Cursor mode.

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

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

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

Automatic Mouse Synchronization

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

Mouse Synchronization Options

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

Menu Option	Description
Absolute	When connected to selected Dominion devices and targets with USB ports, the application will use absolute coordinates to keep the pointers in sync.
Intelligent	Under certain conditions, the application can detect the target mouse settings and synchronize the mouse pointers accordingly, accelerating the mouse on the target device. See ***Intelligent Mouse Synchronization Conditions*** (on page 149) for more details.
Standard	This is the standard mouse synchronization algorithm.

Note: The Intelligent and Standard mouse modes are only available to users working on Dominion devices.

Intelligent Mouse Synchronization Conditions

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

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

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

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

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

Connection and Video Properties

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

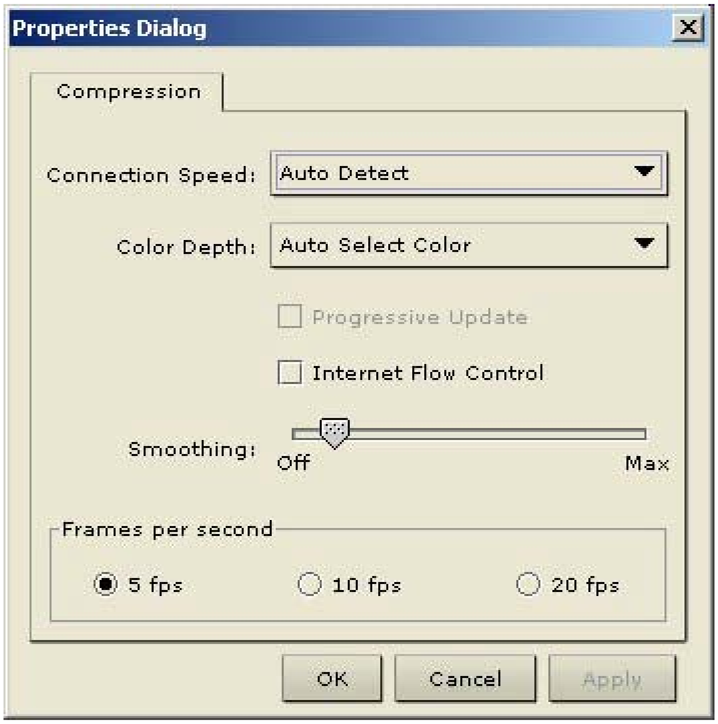
The parameters discussed in this section can be optimized in the Connection Properties dialog and Video Settings dialog.

MPC Connection and Video Properties

Connections

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

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



Connection Speed: Auto Detect

Color Depth: Auto Select Color

□ Progressive Update

□ Internet Flow Control

Smoothing: Off — Max

Frames per second

● 5 fps ○ 10 fps ○ 20 fps

2. Connection Speed - Use this setting to manually adjust the connection speed to accommodate bandwidth constraints. IP-Reach and Dominion can automatically detect available bandwidth and not limit bandwidth use, but you can also adjust this usage according to your needs. Depending on the Raritan device in use, different options may be available.
   - Auto Detect
   - 1G Ethernet
   - 100mb Ethernet
   - 10mb Ethernet
   - 1.5mb (Max DSL/T1)
   - 1mb (Fast DSL/T1)
   - 512 kb (Medium DSL/T1)
   - 384 kb (Slow DSL/T1)
   - 256 kb (Cable)
   - 128 kb (Dual ISDN)
   - 56 kb (ISP Modem)
   - 33 kb (Fast Modem)
   - 24 kb (Slow Modem)
3. Color Depth - IP-Reach and Dominion can dynamically adapt the color depth transmitted to remote users in order to maximize usability in all bandwidths. Select from among the options in the drop-down list (depending on the Raritan device in use, different options may be available):
   - 15-bit RGB Color
   - 8-bit RGB Color
   - 4-bit Color
   - 4-bit Gray
   - 3-bit Gray
   - 2-bit Gray
   - Black and White
   - For information on Progressive Update, Internet Flow Control, Smoothing (15-bit mode only), and Frames per second (MPC only), refer to ***Connection Profiles*** (on page 127).

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

4. Click OK to change the Connection Properties.

Video Properties

Refreshing Video Settings

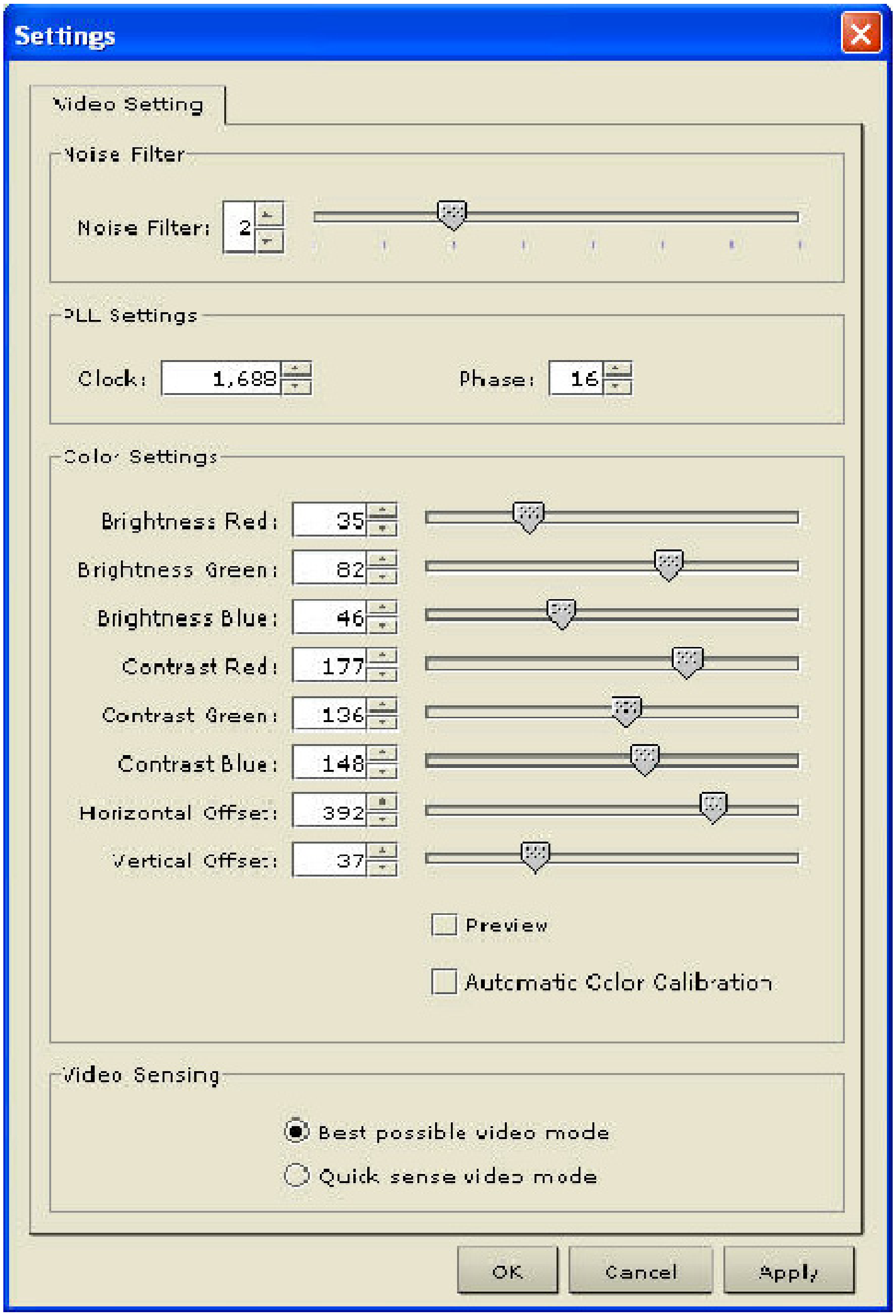
Video settings can be refreshed in several ways:

- Using Video > Refresh Screen.
- Directing the device to automatically detect the video settings (Video > Auto-sense Video Settings).
- Using the ***Color Calibration*** (on page 159) command to calibrate the video, thereby enhancing the colors that are displayed.
- Changing the settings from the Video Settings dialog.

Change Video Settings

➢ ***To change the video settings:***

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



Noise Filter

Noise Filter: 2

PLL Settings

Clock: 1,688

Phase: 16

Color Settings

Brightness Red: 35

Brightness Green: 82

Brightness Blue: 46

Contrast Red: 177

Contrast Green: 136

Contrast Blue: 148

Horizontal Offset: 392

Vertical Offset: 37

□ Preview

□ Automatic Color Calibration

Video Sensing

● Best possible video mode

○ Quick sense video mode

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

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

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

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

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

4. Color Settings - These settings control the brightness, contrast, and positioning of the target server display.

   - Brightness Red - Controls the brightness of the red signal; range is 0 - 127.
   - Brightness Green - Controls the brightness of the green signal; range is 0 - 127.
   - Brightness Blue - Controls the brightness of the blue signal; range is 0 - 127.
   - Contrast Red - Controls the red signal contrast; range is 0 - 255.
   - Contrast Green - Controls the green signal contrast; range is 0 - 255.

- Contrast Blue - Controls the blue signal contrast; range is 0 - 255.
- Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor; range is 0 - 512.
- Vertical Offset - Controls the vertical positioning of the target server display on your monitor; range is 0 - 128.

5. To preview the change prior to making the selection, check the Preview checkbox.
6. Check the Automatic Color Calibration checkbox to enable this feature.
7. Select the video sensing mode:
   - Best possible video mode - IP-Reach or Dominion will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.
   - Quick sense video mode - Selecting this option will cause IP-Reach or Dominion to use a quick video Auto Sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.
8. Click OK to change the Video Settings.

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

Video Settings (Generation 1 Equipment Only)

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

   These settings can be refreshed using the Color Calibration command, described in the next section, by manually forcing IP-Reach or Dominion to autodetect the video settings (on the Video menu, click Auto-sense Video Settings), or by changing the settings in this page. After you change a value, click Apply to test the setting.
2. Noise Filter - IP-Reach or Dominion can filter out electrical interference of video output from graphics cards. This feature optimizes picture quality and reduced used bandwidth.

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

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

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

3. Analog-to-Digital Settings - The following parameters are best left to IP-Reach or Dominion to automatically detect (on the RRC menu bar, select Video > Auto-sense Video Settings), but a brief description of each is included here.
4. PLL Settings - If the video image looks extremely blurry or unfocused, the PLL Settings for clock and phase can be adjusted until a better image appears on the active target server.
   - Clock - Horizontal sync divider to produce pixel clock. Controls how quickly video pixels are displayed across the video page. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended.
   - Phase - Phase values range from 0 to 31 and will wrap around. Stop at the phase value that results in the best video image for the active target server.
5. Color Settings - Gain control can be thought of as contrast adjustment. Offset control can be thought of as brightness adjustment.
   - Red Gain - Controls the amplification of the red signal.
   - Red Offset - Controls the bias of the red signal.
   - Green Gain - Controls the amplification of the green signal.
   - Green Offset - Controls the bias of the green signal.
   - Blue Gain - Controls the amplification of the blue signal.
   - Blue Offset - Controls the bias of the blue signal.

- Link Color Controls - Makes all gain slide adjusters move in unison when any one color's gain slide is moved and all the offset slide adjusters move in unison when any one color's offset slide is moved.

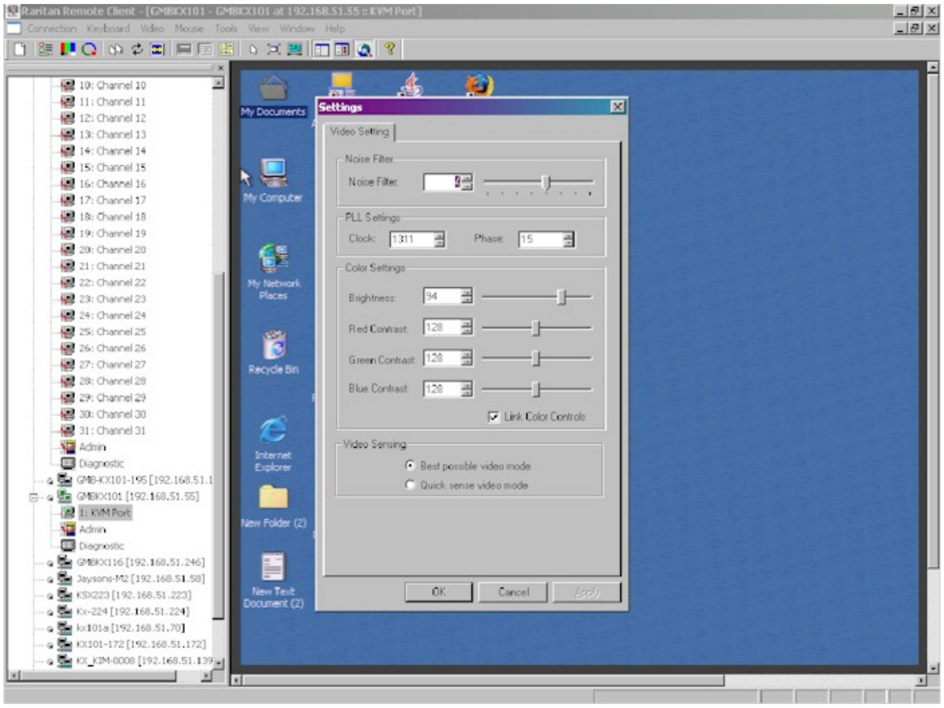
6. Select the video sensing option you would like to apply.

   - Best possible video mode - IP-Reach or Dominion will perform the full Auto Sense process when switching targets or target resolutions. Selecting this radio button will cause IP-Reach or Dominion to calibrate the video for the best image quality.
   - Quick sense video mode - Selecting this radio button will cause IP-Reach or Dominion to use a quick video Auto Sense in order to show the target's video sooner. This option is especially useful for entering a target server's BIOS configuration right after a reboot.

7. Click OK to set Video Settings.

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

Video Settings (KX101 Only)


Raritan Remote Client - [GMBKX101 - GMBKX101 at 192.168.51.55 :: KVM Port]

Settings

Video Setting

Noise Filter

Noise Filter:

PLL Settings

Clock: 1311

Phase: 15

Color Settings

Brightness: 94

Red Contrast: 128

Green Contrast: 128

Blue Contrast: 128

☑ Link Color Controls

Video Sensing

● Best possible video mode

○ Quick sense video mode

Raritan's Dominion KX101 Color Settings dialog varies from those of other Dominion devices.

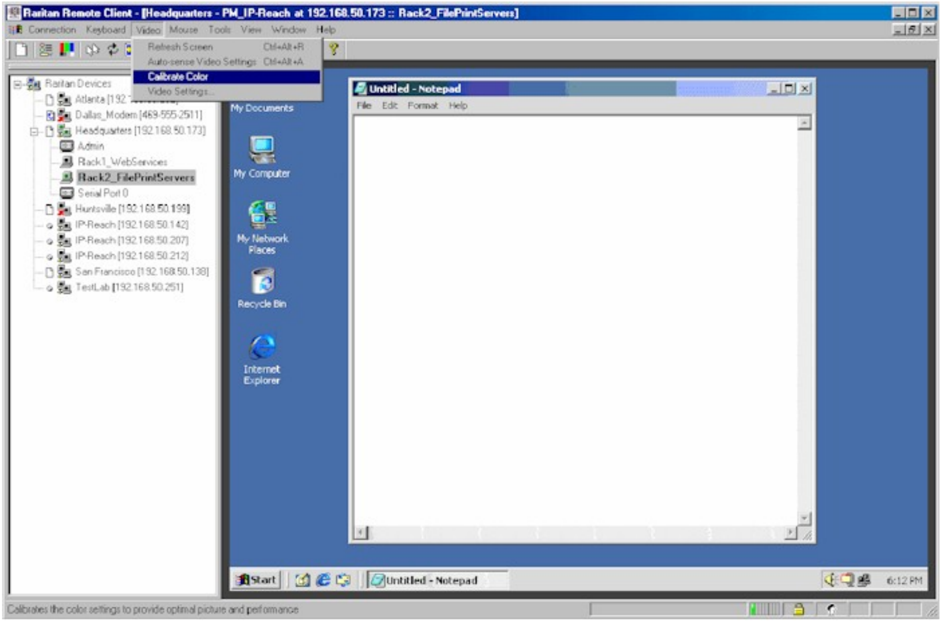
1. In the Color Settings panel, adjust the following options:
   - Brightness - Controls the backlight on your page.
   - Red Contrast - Controls the level of red tone on your page.
   - Green Contrast - Controls the level green tone on your page.
   - Blue Contrast - Controls the level of blue tone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

Color Calibration

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

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

TIP: Open Microsoft Notepad and maximize the window.


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

Tip: You can also specify automatic color calibration using Tools > Options. Refer to ***General Options in MPC*** (on page 161)for more information.

Administrative Functions

Although your device provides a remote interface to administrative functions through device manager, the client provides an interface to frequently-used administrative functions directly from its own interface. When logged into a device as an administrator, you can perform the administrative tasks discussed here.

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

Note to MPC Users

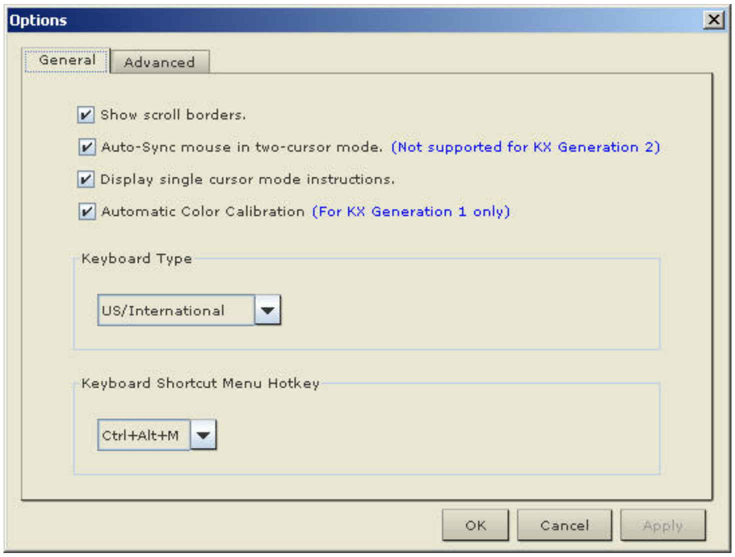
MPC users must belong to the Administrator group in order to receive administrative permissions. MPC uses one permission: either Administrator or Normal User. It is only when the user belongs to the Administrator group that they have access to backup, restore, and restart functions. This is true regardless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

General Options in MPC

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

➢ To configure the general options in MPC:

1. Choose Tools > Options. The Options dialog appears and displays the General tab by default.



☑ Show scroll borders.

☑ Auto-Sync mouse in two-cursor mode. (Not supported for KX Generation 2)

☑ Display single cursor mode instructions.

☑ Automatic Color Calibration (For KX Generation 1 only)

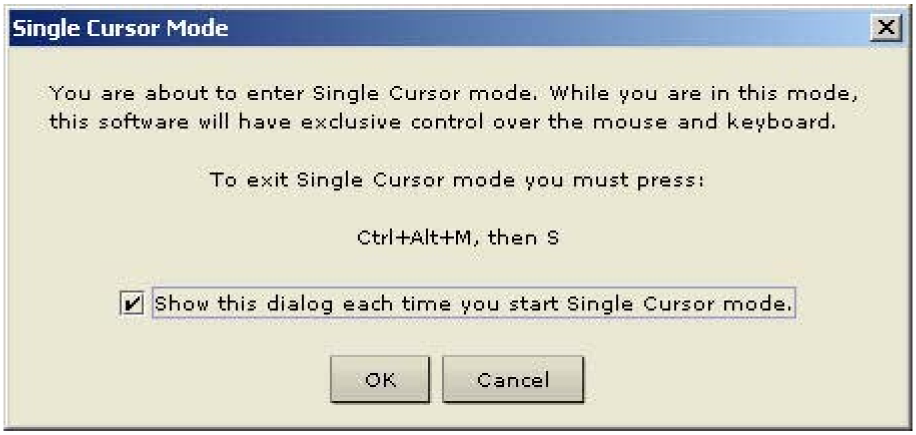
Keyboard Type: US/International

Keyboard Shortcut Menu Hotkey: Ctrl+Alt+M

2. Select the "Show scroll borders" checkbox to view the thin scroll borders designating the autoscroll area.

3. Select the "Auto-Sync mouse in two-cursor mode" checkbox to enable automatic mouse synchronization.

4. If you select the "Display single cursor mode instructions" checkbox, the Single Cursor Mode dialog will appear each time Single Cursor is enabled in the application. See ***Single Mouse Mode/Dual Mouse Mode*** (on page 147) for more information.



You are about to enter Single Cursor mode. While you are in this mode, this software will have exclusive control over the mouse and keyboard.

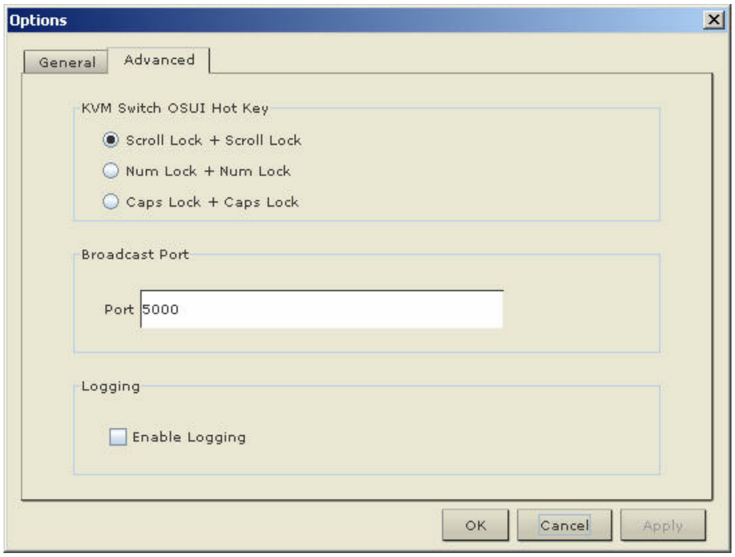
To exit Single Cursor mode you must press:

Ctrl+Alt+M, then S

☑ Show this dialog each time you start Single Cursor mode.

5. Select the Automatic Color Calibration checkbox to enable automatic color calibration. This option is available for KX generation 1 (G1) only.
6. Select the Keyboard Type from the drop-down list (depending on the Raritan device in use, different options may be available):
   - US/International
   - French (France)
   - German (Germany)
   - Japanese
   - United Kingdom
   - Korean (Korea)
   - Belgian
   - Norwegian
7. From the Keyboard Shortcut Menu HotKey drop-down, select the key combination you would like to use to invoke the ***Shortcut Menu*** (on page 138).

8. For advanced options, open the Advanced tab.



Options

General | Advanced

KVM Switch OSUI Hot Key

● Scroll Lock + Scroll Lock

○ Num Lock + Num Lock

○ Caps Lock + Caps Lock

Broadcast Port

Port 5000

Logging

□ Enable Logging

9. From the KVM Switch OSUI Hot Key section, select the hot key to use when switching between target server displays.

10. For the Broadcast Port, type the broadcast port number in the Port field if you want to use a port other then 5000.

11. Select the Enable Logging checkbox only if directed to by Technical Support. This option creates a log file in your home directory.

12. Click OK when finished. Click Apply any time while making selections to apply it.

Upgrading Device Firmware

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

1. Connect to the device by highlighting the device's icon in the Navigator.

2. Click Tools > Update > Update Device to perform firmware upgrades.

3. You will be prompted to locate a Raritan firmware distribution file (*.RFP format), which can be found on the Raritan website (www.raritan.com) on the Firmware Upgrades page.

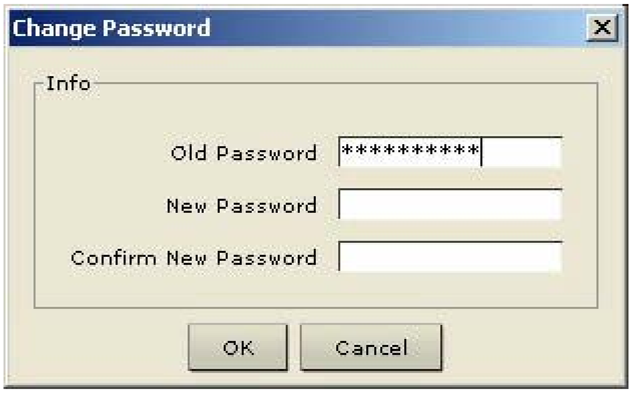
Ensure that you read all instructions included in firmware ZIP files carefully before upgrading a device.

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

Changing a Password

➢ **To update your password**

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



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

Restarting a Device

➢ **To restart a device:**

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

Backing Up a Device Configuration

➢ **To back up a device:**

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

Restoring a Device Configuration

- ***To restore a device configuration:***

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

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

Backing Up a User Configuration

- ***To back up a device's user configuration:***

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

Restoring a User Configuration

- ***To restore a user configuration:***

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

Note: Use these commands to easily transfer user and group information from one device to another.

Log Files

Activity Log

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

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

Broadcast Port

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

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

1. Select the device in the Navigator.

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

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

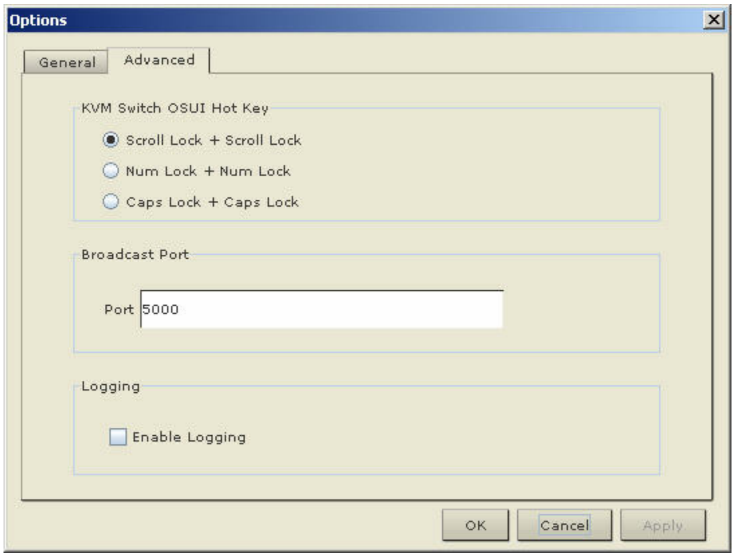
MPC Broadcast Port

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

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

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

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



KVM Switch OSUI Hot Key
● Scroll Lock + Scroll Lock
○ Num Lock + Num Lock
○ Caps Lock + Caps Lock

Broadcast Port
Port 5000

Logging
□ Enable Logging

Remote Power Management

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

- Power On
- Power Off
- Cycle Power

➢ To change the power status of a target:

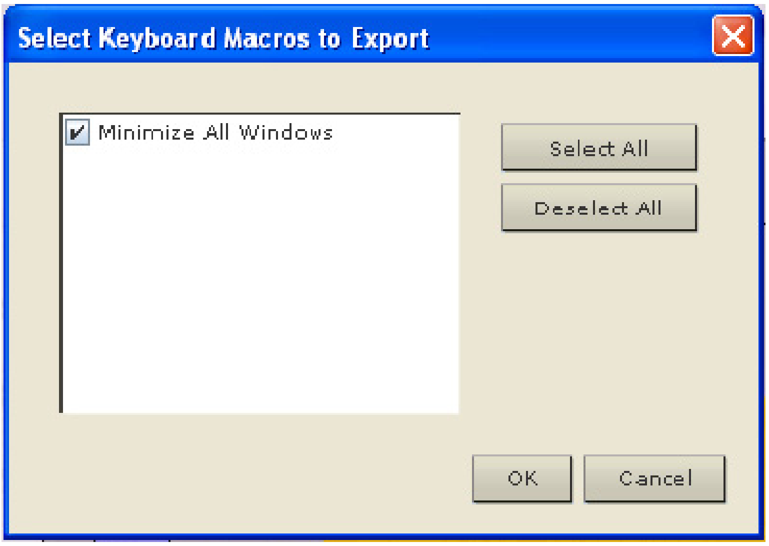
1. Select the device in the Navigator.
2. On the Tools menu, choose Power On, Power Off, or Cycle Power.

Import/Export MPC Keyboard Macros

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

➢ To export MPC macros:

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

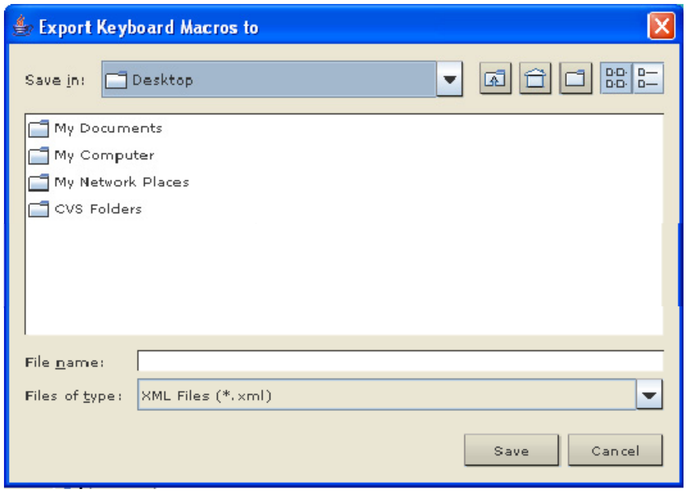


2. Select the macros to be exported by checking their corresponding checkbox or using the Select All or Deselect All options.

3. Click OK. The selected macro file(s) will be moved to your desktop (by default).

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

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



➢ ***To import MPC macros:***

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

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

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

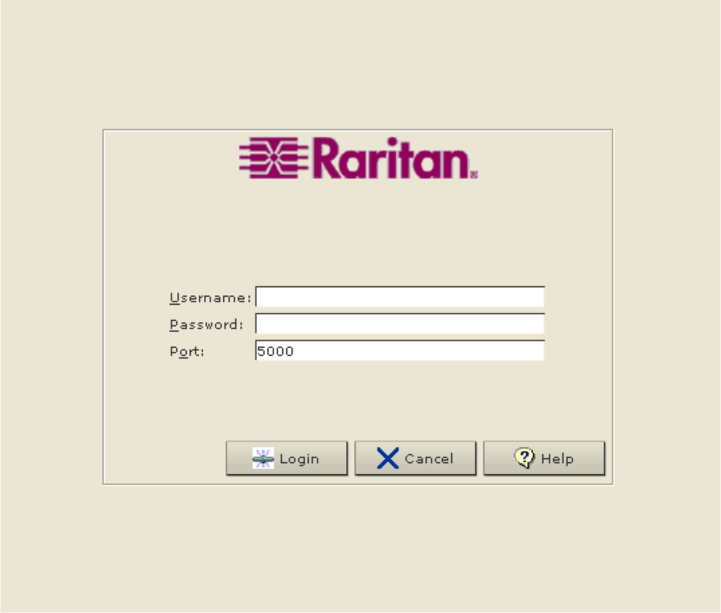
The macros will then be imported.

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

Opening Administrator and Diagnostic Interfaces

Administrator Interface

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



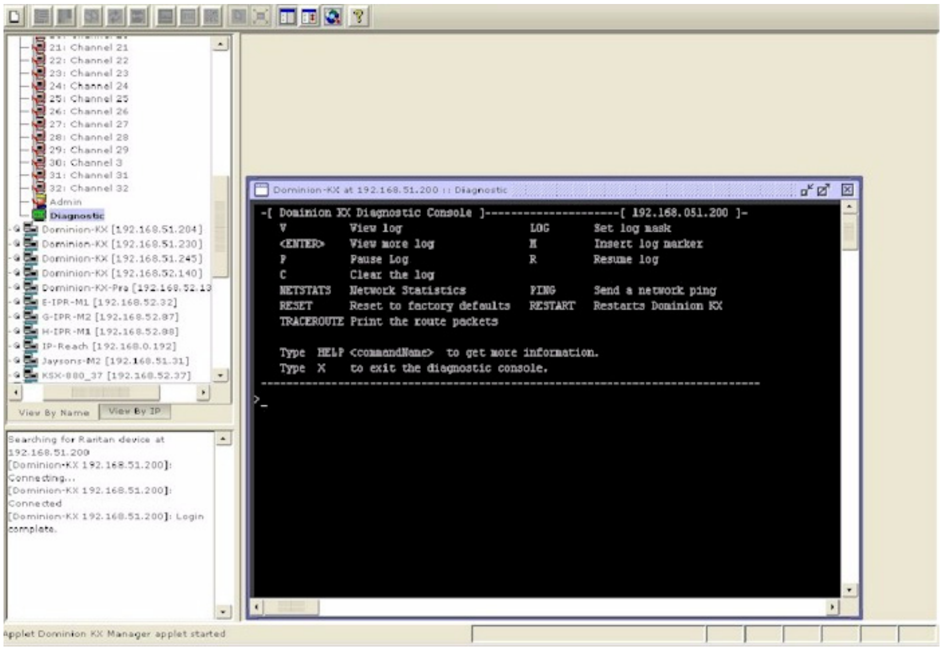
Username:

Password:

Port: 5000

Diagnostic Interface (excluding Dominion KX II)

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



```
Searching for Raritan device at
192.168.51.200
[Dominion-KX 192.168.51.200]:
Connecting...
[Dominion-KX 192.168.51.200]:
Connected
[Dominion-KX 192.168.51.200]: Login
complete.
```

```
-[ Dominion KX Diagnostic Console ]--------------------[ 192.168.051.200 ]-
   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 KX
   TRACEROUTE Print the route packets

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

Applet Dominion KX Manager applet started

Chapter 4 Virtual Media

In This Chapter

Overview

Virtual media extends KVM capabilities by enabling KVM target servers to remotely access media from the client PC and network file servers. With this feature, media mounted on the client PC and network file servers is essentially "mounted virtually" by the target server. The target server can then read from and write to that media as if it were physically connected to the target server itself. Virtual media can include internal and USB-mounted CD and DVD drives, USB mass storage devices, PC hard drives, and ISO images (disk images).

Note: ISO9660 is the standard supported by Raritan. However, other ISO standards can be used.

Virtual media provides the ability to perform additional tasks remotely, such as:

- Transferring files
- Running diagnostics
- Installing or patching applications
- Complete installation of the operating system

This expanded KVM control eliminates most trips to the data center, saving time and money, thereby making virtual media very powerful.

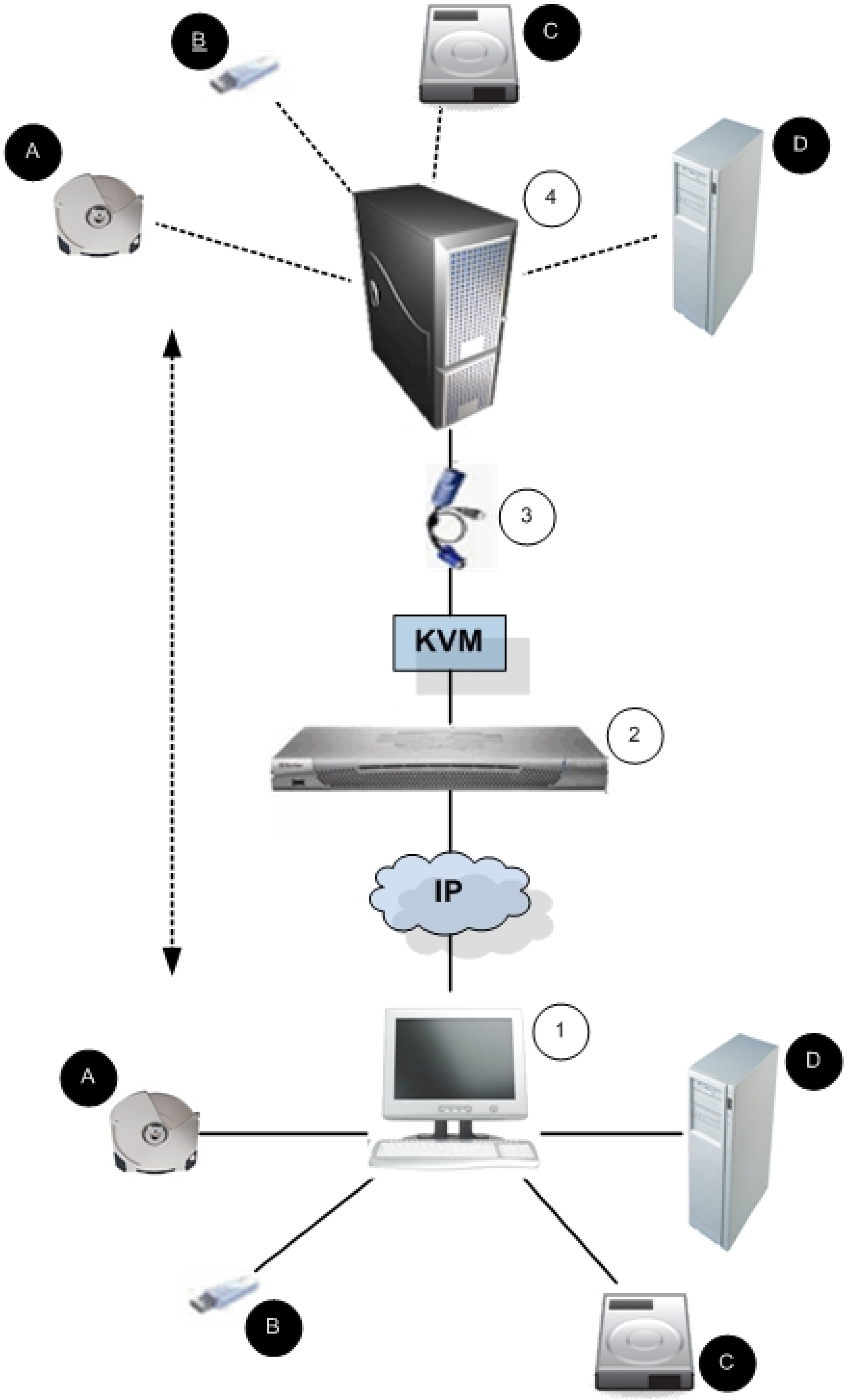

B
C
A
D
4
3
KVM
2
IP
1
A
D
B
C

Diagram key			
①	Desktop PC	🅐	CD/DVD drive
②	Dominion KX II	🅑	USB
③	CIM	🅒	Hard drive image files
④	Target server	🅓	Remote file server (ISO images)

Prerequisites for Using Virtual Media

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

Dominion KX II

- For users requiring access to virtual media, the Dominion KX II permissions must be set to allow access to the relevant ports, as well as virtual media access (VM Access port permission) for those ports. Port permissions are set at the group-level; refer to ***Setting Port Permissions*** (on page 200) in the device user guide for more information.
- A USB connection must exist between the Dominion KX II device and the target server.
- If you want to use PC-Share, ***Security Settings*** (on page 248) must also be enabled in the Security Settings page. **Optional**
- You must choose the correct USB profile for the KVM target server you are connecting to.

Client PC

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

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

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

Target Server

- KVM target servers must support USB connected drives.
- KVM target servers running Windows 2000 must have all of the recent patches installed.
- USB 2.0 ports are both faster and preferred.

File Server Setup (File Server ISO Images Only)

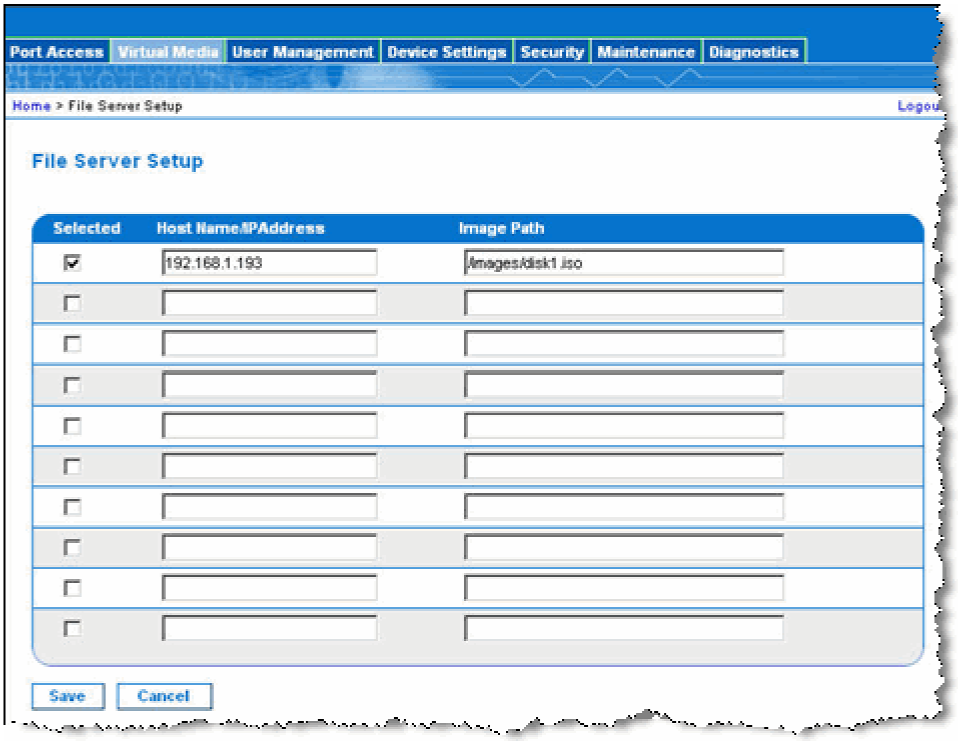
Note: This feature is only required when using virtual media to access file server ISO images.

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

Use the Dominion KX II Remote Console File Server Setup page to designate the files server(s) and image paths that you want to access using Dominion KX II virtual media. File server ISO image(s) specified here will become available for selection in the Remote Server ISO Image Hostname and Image drop-down lists in the Map Virtual Media CD/ISO Image dialog. See ***CD-ROM/DVD-ROM/ISO Images*** (on page 183).

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

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



Selected	Host Name/IPAddress	Image Path
☑	192.168.1.193	/images/disk1.iso
☐		
☐		
☐		
☐		
☐		
☐		
☐		
☐		
☐		

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

- Host Name/IP Address. Host name or IP address of the file server.
- Image Path. Full path name of the location of the ISO image.

3. Check the Selected checkbox for all media that you want accessible as virtual media.
4. Click Save. All media specified here will now be available for selection in the Map Virtual Media CD/ISO Image dialog.

Using Virtual Media

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

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

➢ ***To use virtual media:***

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

Verify that the appropriate prerequisites are met. See ***Prerequisites for Using Virtual Media*** (on page 175).

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

Dominion KX II

- For users requiring access to virtual media, Dominion KX II permissions must be set to allow access to the relevant ports, as well as virtual media access (VM Access port permission) for those ports. Port permissions are set at the group-level; refer to ***Setting Port Permissions*** (on page 200) in the device user guide for more information.
- A USB connection must exist between the Dominion KX II device and the target server.
- If you want to use PC-Share, ***Security Settings*** (on page 248) must also be enabled in the Security Settings page. **Optional**
- You must choose the correct USB profile for the KVM target server you are connecting to.

Client PC

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

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

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

Target Server

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

1. USB 2.0 ports are both faster and preferred..
2. If you plan to access file server ISO images, identify those file servers and images through the Dominion KX II Remote Console File Server Setup page. See ***File Server Setup (File Server ISO Images Only)*** (on page 177).

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

3. Open a KVM session with the appropriate target server.

a. Open the Port Access page from the Dominion KX II Remote Console.

b. Connect to the target server from the Port Access page:

- Click the Port Name for the appropriate server.
- Choose the Connect command from the Port Action menu. The target server opens in a ***Virtual KVM Client*** (on page 50) window.

4. Connect to the virtual media.

For:	Select this VM option:
Local drives	***Connect Drive*** (see "Local Drives" on page 181)
Local CD/DVD drives	***Connect CD-ROM/ISO Image*** (see "CD-ROM/DVD-ROM/ISO Images" on page 183)
ISO Images	Connect CD-ROM/ISO Image
File Server ISO Images	Connect CD-ROM/ISO Image

5. Upon completion of your tasks, disconnect the virtual media. See ***Disconnecting Virtual Media*** (on page 184).

Connecting to Virtual Media

Local Drives

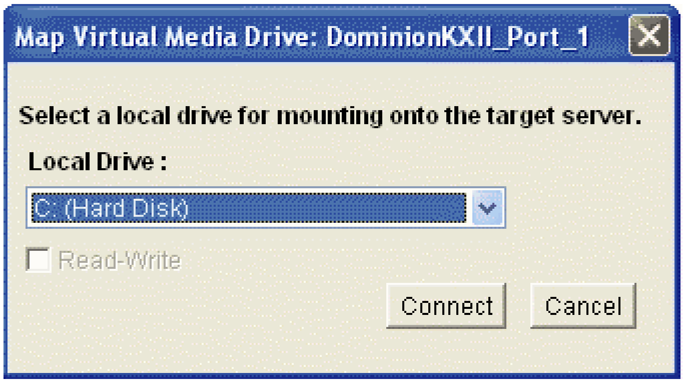
This option mounts an entire drive, which means the entire disk drive is mounted virtually onto the target server. Use this option for hard drives and external drives only; it does not include network drives, CD-ROM, or DVD-ROM drives. This is the only option for which Read/Write is available.

Note: KVM target servers running certain versions of the Windows operating system may not accept new mass storage connections after an NTFS-formatted partition (for example, the local C drive) has been redirected to them.

If this occurs, close the Dominion KX II Remote Console and reconnect before redirecting another virtual media device. If other users are connected to the same target server, they must also close their connections to the target server.

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

1. From the Virtual KVM Client, choose Virtual Media > Connect Drive. The Map Virtual Media Drive dialog appears.



Map Virtual Media Drive: DominionKXII_Port_1

Select a local drive for mounting onto the target server.

Local Drive : C: (Hard Disk)

□ Read-Write

2. Choose the drive from the Local Drive drop-down list.
3. If you want Read and Write capabilities, select the Read-Write checkbox. This option is disabled for nonremovable drives. Refer to the ***Conditions when Read/Write is Not Available*** (on page 182) for more information. When checked, you will be able to read or write to the connected USB disk.

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

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

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

Conditions when Read/Write is Not Available

Virtual media Read/Write is not available in the following situations:

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

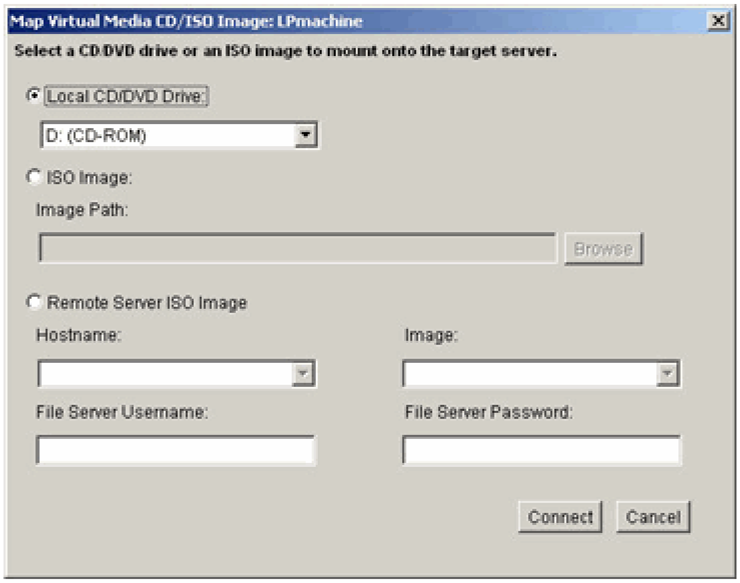
CD-ROM/DVD-ROM/ISO Images

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

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

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

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



Map Virtual Media CD/ISO Image: LPmachine

Select a CD/DVD drive or an ISO image to mount onto the target server.

● Local CD/DVD Drive:

D: (CD-ROM)

○ ISO Image:

Image Path:

○ Remote Server ISO Image

Hostname:

Image:

File Server Username:

File Server Password:

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

d. Click Connect.

4. For remote ISO images on a file server:

   a. Choose the Remote Server ISO Image option.

   b. Choose Hostname and Image from the drop-down lists. The file servers and image paths available are those that you configured using the File Server Setup page. Only items you configured using the Dominion KX II File Server Setup page will be in the drop-down list. Refer to ***File Server Setup (File Server ISO Images Only)*** (on page 177) for more information.

   c. File Server Username. User name required for access to the file server.

   d. File Server Password. Password required for access to the file server (field is masked as you type).

   e. Click Connect.

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

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

Disconnecting Virtual Media

➢ ***To disconnect the virtual media drives:***

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

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

Chapter 5 Configuring USB Profiles

In This Chapter

Overview

To broaden the Dominion KX II's compatibility with different KVM target servers, Raritan provides a standard selection of USB configuration profiles for a wide range of operating system and BIOS-level server implementations.

The Generic (default) USB profile meets the needs of the vast majority of deployed KVM target server configurations. Additional profiles are provided to meet the specific needs of other commonly deployed server configurations (for example, Linux and Mac OS X). There are also a number of profiles (designated by platform name and BIOS revision) to enhance virtual media function compatibility with the target server, for example, when operating at the BIOS level.

USB profiles are configured on the Device Settings > Port Configuration > Port page of the Dominion KX II Remote and Local Consoles. A device administrator can configure the port with the profiles that best meet the needs of the user and the target server configuration.

A user connecting to a KVM target server chooses among these preselected profiles in the ***Virtual KVM Client*** (on page 50), depending on the operational state of the KVM target server. For example, if the server is running and the user wants to use the Windows operating system, it would be best to use the Generic profile. But if the user wants to change settings in the BIOS menu or boot from a virtual media drive, depending on the target server model, a BIOS profile may be more appropriate.

Should none of the standard USB profiles provided by Raritan work with a given KVM target, Raritan Technical Support can provide a custom profile to establish a viable connection to the KVM target. Custom profiles that are useful to a wide range of customers will be included in scheduled firmware upgrades.

CIM Compatibility

In order to make use of USB profiles, you must use a D2-CIM VUSB or D2-CIM DVUSB with updated firmware. A VM-CIM that has not had its firmware upgraded will support a broad range of configurations (Keyboard, Mouse, CD-ROM, and Removable Drive) but will not be able to make use of profiles optimized for particular target configurations. Given this, existing VM-CIMs should be upgraded with latest firmware in order to access USB profiles. Until existing VM-CIMs are upgraded, they will be able to provide functionality equivalent to the 'Generic' profile.

VM-CIM firmware is automatically upgraded during a Dominion KX II firmware upgrade, but VM-CIMs that have not had their firmware upgraded can be upgraded as described in ***Upgrading CIMs*** (on page 264).

See ***Computer Interface Modules (CIMs)*** (on page 295) for additional information.

Available USB Profiles

The current release of the Dominion KX II comes with the selection of USB profiles described in the following table. New profiles are included with each firmware upgrade provided by Raritan. For information about new USB profiles, see the release notes provided with each firmware release.

USB profile	Description
BIOS Dell PowerEdge 1950/2950/2970/6950/R200	Dell PowerEdge 1950/2950/2970/6950/R200 BIOS Use either this profile or 'Generic' profile for Dell PowerEdge 1950/2950/2970/6950/R200 BIOS. Restrictions: None

USB profile	Description
BIOS DellOptiplex Keyboard Only	Dell Optiplex BIOS Access (Keyboard Only) Use this profile to have keyboard functionality for the Dell Optiplex BIOS when using D2CIM-VUSB. When using the new D2CIM-DVUSB, use 'Generic' profile. Notice: Optiplex 210L/280/745/GX620 requires D2CIM-DVUSB with 'Generic' profile to support Virtual Media Restrictions: USB bus speed limited to full-speed (12 MBit/s) No Virtual Media support

Available USB Profiles

USB profile	Description
BIOS DellPowerEdge Keyboard Only	Dell PowerEdge BIOS Access (Keyboard Only) Use this profile to have keyboard functionality for the Dell PowerEdge BIOS when using D2CIM-VUSB. When using the new D2CIM-DVUSB, use 'Generic' profile. Notice: PowerEdge 650/1650/1750/2600/2650 BIOS do not support USB CD-ROM and disk drives as a bootable device PowerEdge 750/850/860/1850/2850/SC1425 BIOS requires D2CIM-DVUSB with 'Generic' profile to support Virtual Media Use 'BIOS Dell PowerEdge 1950/2950/2970/6950/R200' or 'Generic' profile for PowerEdge 1950/2950/2970/6950/R200 when operating in the BIOS Restrictions: USB bus speed limited to full-speed (12 MBit/s) Absolute mouse synchronization™ not supported No Virtual Media support

USB profile	Description
BIOS Generic	BIOS Generic Use this profile when Generic OS profile does not work on the BIOS. WARNING: USB enumeration will trigger whenever Virtual Media is connected or disconnected Restrictions: USB bus speed limited to full-speed (12 MBit/s) Absolute mouse synchronization™ not supported Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS HP Proliant DL145	HP Proliant DL145 PhoenixBIOS Use this profile for HP Proliant DL145 PhoenixBIOS during OS installation. Restrictions: USB bus speed limited to full-speed (12 MBit/s)
BIOS HPCompaq DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 Use this profile to boot the HP Compaq DC7100/DC7600 series desktops from Virtual Media. Restrictions: Virtual CD-ROM and disk drives cannot be used simultaneously

Available USB Profiles

USB profile	Description
BIOS IBM ThinkCentre Lenovo	IBM Thinkcentre Lenovo BIOS Use this profile for the IBM Thinkcentre Lenovo system board (model 828841U) during BIOS operations. Restrictions: USB bus speed limited to full-speed (12 MBit/s) Virtual CD-ROM and disk drives cannot be used simultaneously
BIOS Lenovo ThinkPad T61 & X61	BIOS Lenovo ThinkPad T61 and X61 (boot from Virtual Media) Use this profile to boot the T61 and X61 series laptops from Virtual Media. Restrictions: USB bus speed limited to full-speed (12 MBit/s)
BIOS Mac	BIOS Mac Use this profile for Mac BIOS. Restrictions: Absolute mouse synchronization™ not supported Virtual CD-ROM and disk drives cannot be used simultaneously
Generic	The generic USB profile resembles the behavior of the original KX2 release. Use this for Windows 2000, XP, Vista and later. Restrictions: None

USB profile	Description
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	HP Proliant DL360/DL380 G4 (HP SmartStart CD) Use this profile for the HP Proliant DL360/DL380 G4 series server when installing OS using HP SmartStart CD. Restrictions: USB bus speed limited to full-speed (12 MBit/s) Absolute mouse synchronization™ not supported
HP Proliant DL360/DL380 G4 (Windows 2003 Server Installation)	HP Proliant DL360/DL380 G4 (Windows 2003 Server Installation) Use this profile for the HP Proliant DL360/DL380 G4 series server when installing Windows 2003 Server without the help of HP SmartStart CD. Restrictions: USB bus speed limited to full-speed (12 MBit/s)
Linux	Generic Linux profile This is the generic Linux profile; use it for Redhat Enterprise Linux, SuSE Linux Enterprise Desktop and similar disributions. Restrictions: Absolute mouse synchronization™ not supported

USB profile	Description
MAC OS X (10.4.9 and later)	Mac OS-X, version 10.4.9 and later This profile compensates the scaling of mouse coordinates introduced in recent versions of Mac OS-X. Select this if the remote and local mouse positions get out of sync near the desktop borders. Restrictions: Virtual CD-ROM and disk drives cannot be used simultaneously
RUBY Industrial Mainboard (AwardBIOS)	RUBY Industrial Mainboard (AwardBIOS) Use this profile for the RUBY-9715VG2A series industrial mainboards with Phoenix/AwardBIOS v6.00PG. Restrictions: USB bus speed limited to full-speed (12 MBit/s) Virtual CD-ROM and disk drives cannot be used simultaneously
Supermicro Mainboard Phoenix (AwardBIOS)	Supermicro Mainboard Phoenix AwardBIOS Use this profile for the Supermicro series mainboards with Phoenix AwardBIOS. Restrictions: Virtual CD-ROM and disk drives cannot be used simultaneously

USB profile	Description
Suse 9.2	SuSE Linux 9.2 Use this for SuSE Linux 9.2 disribution. Restrictions: Absolute mouse synchronization™ not supported USB bus speed limited to full-speed (12 MBit/s)
Troubleshooting 1	Troubleshooting Profile 1 Mass Storage first Keyboard and Mouse (Type 1) USB bus speed limited to full-speed (12 MBit/s) Virtual CD-ROM and disk drives cannot be used simultaneously WARNING: USB enumeration will trigger whenever Virtual Media is connected or disconnected.
Troubleshooting 2	Troubleshooting Profile 2 Keyboard and Mouse (Type 2) first Mass Storage USB bus speed limited to full-speed (12 MBit/s) Virtual CD-ROM and disk drives cannot be used simultaneously WARNING: USB enumeration will trigger whenever Virtual Media is connected or disconnected.

USB profile	Description
Troubleshooting 3	Troubleshooting Profile 3 Mass Storage first Keyboard and Mouse (Type 2) USB bus speed limited to full-speed (12 MBit/s) Virtual CD-ROM and disk drives cannot be used simultaneously WARNING: USB enumeration will trigger whenever Virtual Media is connected or disconnected.
Use Full Speed for Virtual Media CIM	Use Full Speed for Virtual Media CIM This profile resembles the behavior of the original KX2 release with Full Speed for Virtual Media CIM option checked. Useful for BIOS that cannot handle High Speed USB devices. Restrictions: USB bus speed limited to full-speed (12 MBit/s)

Selecting Profiles for a KVM Port

The Dominion KX II comes with a set of USB profiles that you assign to a KVM port based on the characteristics of the KVM target server it connects to. You assign USB profiles to a KVM port in the Device Settings > Port Configuration > Port page in either the Dominion KX II Remote or Local Console.

It is the administrator that designates the profiles that are most likely to be needed for a specific target. These profiles are then available for selection via MPC/VKC. If a profile has not been made available, you can access any of the available profiles by selecting USB Profile > Other Profiles.

Assigning USB profiles to a KVM port makes those profiles available to a user when connected to a KVM target server. The user selects a USB profile from the USB Profile menu in VKC.

For information about assigning USB profiles to a KVM port, see ***USB Profiles (Port page)*** (on page 243).

Chapter 6 User Management

In This Chapter

User Groups

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

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

User	Description
Admin	Users that are members of this group have full administrative privileges. The original, factory-default user is a member of this group and has the complete set of system privileges. In addition, the Admin user must be a member of the Admin group.
Unknown	This is the default group for users who are authenticated externally using LDAP/LDAPS or RADIUS or who are unknown to the system. If the external LDAP/LDAPS or RADIUS server does not identify a valid user group, the Unknown group is used. In addition, any newly created user is automatically put in this group until assigned to another group.
Individual Group	An individual group is essentially a "group" of one. That is, the specific user is in its own group, not affiliated with other real groups. Individual groups can be identified by the "@" in the Group Name. The individual group allows a user account to have the same rights as a group.

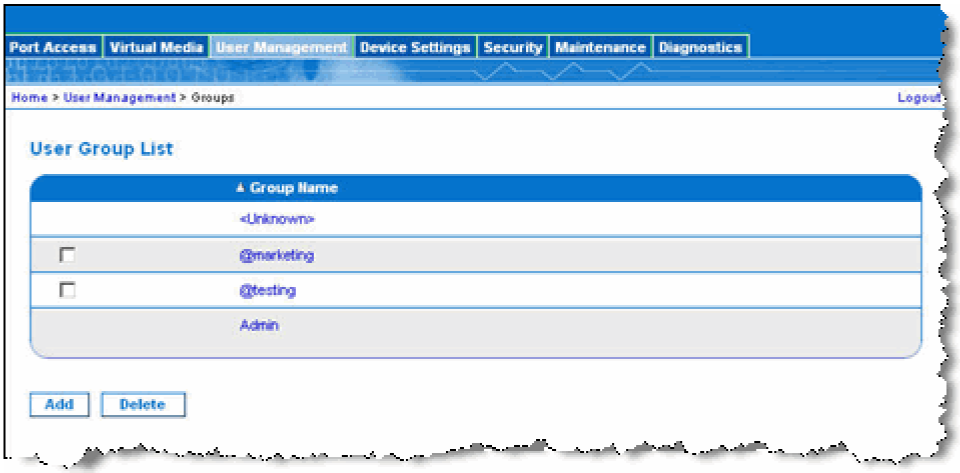
User Group List

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

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

➢ *To list the user groups:*

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



User Group List

	▲ Group Name
	<Unknown>
□	@marketing
□	@testing
	Admin

Relationship Between Users and Groups

Users belong to a group and groups have privileges. Organizing the various users of your Dominion KX II into groups saves time by allowing you to manage permissions for all users in a group at once, instead of managing permissions on a user-by-user basis.

You may also choose not to associate specific users with groups. In this case, you can classify the user as "Individual."

Upon successful authentication, the device uses group information to determine the user's permissions, such as which server ports are accessible, whether rebooting the device is allowed, and other features.

Users, Groups, and Access Permissions

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

Adding a New User Group

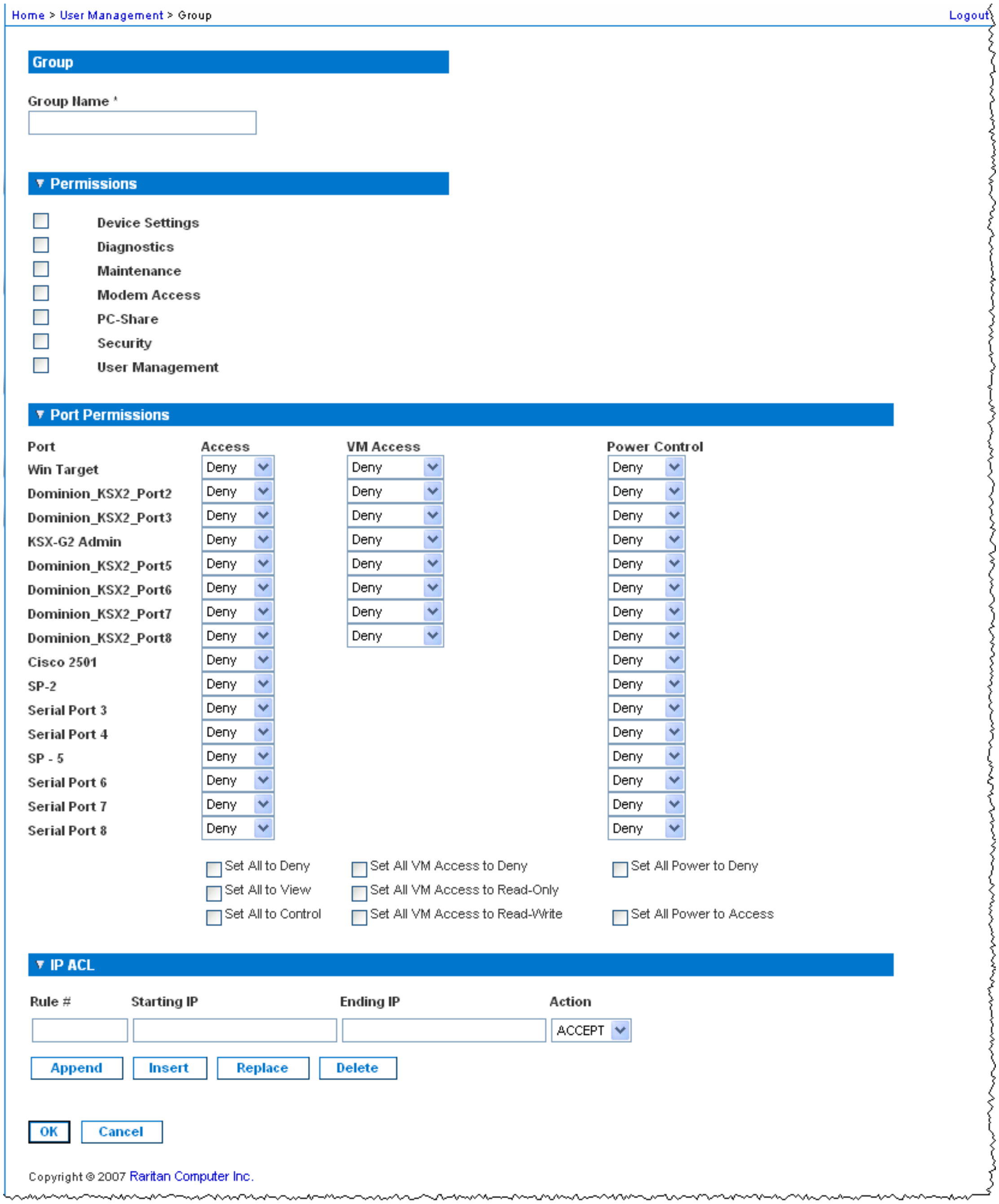
➢ ***To add a new user group:***

1. Open the Group page by selecting User Management > Add New User Group or clicking the Add button from the User Group List page.

   The Group page is organized into the following categories: Group, Permissions, Port Permissions, and IP ACL.

2. Type a descriptive name for the new user group into the Group Name field.
3. Set the permissions for the group. Select the checkboxes before the permissions you want to assign to all of the users belonging to this group. Refer to ***Setting Permissions*** (on page 200) for more information.
4. Set the port permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). Refer to ***Setting Port Permissions*** (on page 200) for more information.
5. Set the IP ACL. Refer to ***Group-based IP ACL (Access Control List)*** (on page 201) for more information. This feature limits access to the Dominion KX II device by specifying IP addresses. It applies only to users belonging to a specific group, unlike the ***IP Access Control*** (on page 256) list feature that applies to all access attempts to the device (and takes priority). **Optional**
6. Click OK.

Note: Several administrative functions are available within MPC and from the Dominion KX II Local Console. These functions are available only to members of the default Admin group.



Group

Group Name *

▼ Permissions

□ Device Settings
□ Diagnostics
□ Maintenance
□ Modem Access
□ PC-Share
□ Security
□ User Management

▼ Port Permissions

Port	Access	VM Access	Power Control
Win Target	Deny	Deny	Deny
Dominion_KSX2_Port2	Deny	Deny	Deny
Dominion_KSX2_Port3	Deny	Deny	Deny
KSX-G2 Admin	Deny	Deny	Deny
Dominion_KSX2_Port5	Deny	Deny	Deny
Dominion_KSX2_Port6	Deny	Deny	Deny
Dominion_KSX2_Port7	Deny	Deny	Deny
Dominion_KSX2_Port8	Deny	Deny	Deny
Cisco 2501	Deny		Deny
SP-2	Deny		Deny
Serial Port 3	Deny		Deny
Serial Port 4	Deny		Deny
SP - 5	Deny		Deny
Serial Port 6	Deny		Deny
Serial Port 7	Deny		Deny
Serial Port 8	Deny		Deny

□ Set All to Deny
□ Set All to View
□ Set All to Control

□ Set All VM Access to Deny
□ Set All VM Access to Read-Only
□ Set All VM Access to Read-Write

□ Set All Power to Deny
□ Set All Power to Access

▼ IP ACL

Rule #	Starting IP	Ending IP	Action
			ACCEPT

Copyright © 2007 Raritan Computer Inc.

Setting Permissions

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

Permission	Description
Device Settings	Network settings, date/time settings, port configuration (channel names, power associations), event management (SNMP, Syslog), virtual media file server setup
Diagnostics	Network interface status, network statistics, ping host, trace route to host, Dominion KX II diagnostics
Maintenance	Backup and restore database, firmware upgrade, factory reset, reboot
Modem Access	Permission to use the modem to connect to the KSX device.
PC-Share	Simultaneous access to the same target by multiple users
Security	SSL certificate, security settings (VM Share, PC-Share), IP ACL
User Management	User and group management, remote authentication (LDAP/LDAPS/RADIUS), login settings

Setting Port Permissions

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

Access		VM access		Power control	
Option	Descrip.	Option	Descrip.	Option	Descrip.

Access		VM access		Power control	
None*	Denied access completely	Deny*	Virtual media permission is denied altogether for the port	Deny*	Deny power control to the target server
View	View the video (but not interact with) the connected target server	Read-Only	Virtual media access is limited to read access only	Access	Full permission to power control on a target server
Control	Control the connected target server	Read-Write	Complete access (read, write) to virtual media		

* Default setting

Tip: Use the checkboxes to quickly set all the permissions the same for every port.

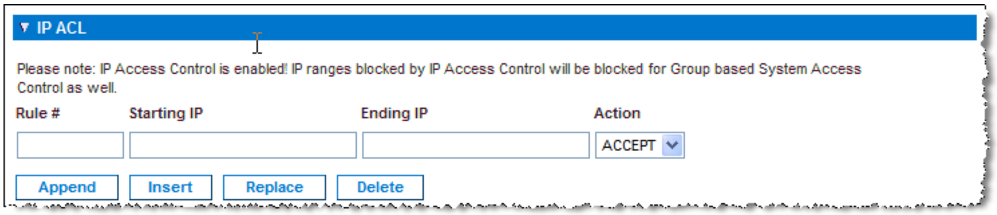
Group-Based IP ACL (Access Control List)

Important: Exercise caution when using group-based IP access control. It is possible to be locked out of your Dominion KX II if your IP address is within a range that has been denied access.

This feature limits access to the Dominion KX II device by users in the selected group to specific IP addresses. This feature applies only to users belonging to a specific group, unlike the IP Access Control List feature that applies to all access attempts to the device, is processed first, and takes priority. Refer to ***IP Access Control*** (on page 256) for more information.

Important: The IP address 127.0.0.1 is used by the Dominion KX II Local Port and cannot be blocked.

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



Please note: IP Access Control is enabled! IP ranges blocked by IP Access Control will be blocked for Group based System Access Control as well.

➢ *To add (append) rules:*

1. Type the starting IP address in the Starting IP field.
2. Type the ending IP address in the Ending IP field.
3. Choose the action from the available options:
   - Accept - IP addresses set to Accept are allowed access to the Dominion KX II device.
   - Drop - IP addresses set to Drop are denied access to the Dominion KX II device.
4. Click Append. The rule is added to the bottom of the rules list. Repeat steps 1 through 4 for each rule you want to enter.

➢ *To insert a rule:*

1. Enter a rule #. A rule # is required when using the Insert command.
2. Enter the Starting IP and Ending IP fields.
3. Choose the action from the Action drop-down list.
4. Click Insert. If the rule # you just typed equals an existing rule #, the new rule is placed ahead of the exiting rule and all rules are moved down in the list.

➢ *To replace a rule:*

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

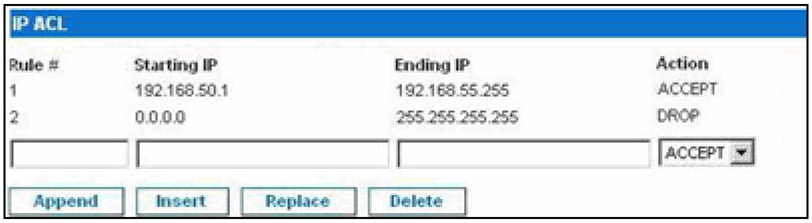
➢ *To delete a rule:*

1. Specify the rule # you want to delete.

2. Click Delete.

3. When prompted to confirm the deletion, click OK.

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



IP ACL

Rule #	Starting IP	Ending IP	Action
1	192.168.50.1	192.168.55.255	ACCEPT
2	0.0.0.0	255.255.255.255	DROP

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

Setting Permissions for an Individual Group

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

1. Locate the group from among the groups listed. Individual groups can be identified by the @ in the Group Name.

2. Click the Group Name. The Group page opens.

3. Select the appropriate permissions.

4. Click OK.

Modifying an Existing User Group

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

➢ ***To modify an existing user group:***

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

2. Set the Permissions for the group. Select the checkboxes before the permissions you want to assign to all of the users belonging to this group. Refer to *Setting Permissions* (on page 200) for more information.

3. Set the Port Permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). Refer to ***Setting Port Permissions*** (on page 200) for more information.
4. Set the IP ACL (optional). This feature limits access to the Dominion KX II device by specifying IP addresses. Refer to ***Group-based IP ACL (Access Control List)*** (on page 201) for more information.
5. Click OK.

➢ ***To delete a user group:***

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

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

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

Users

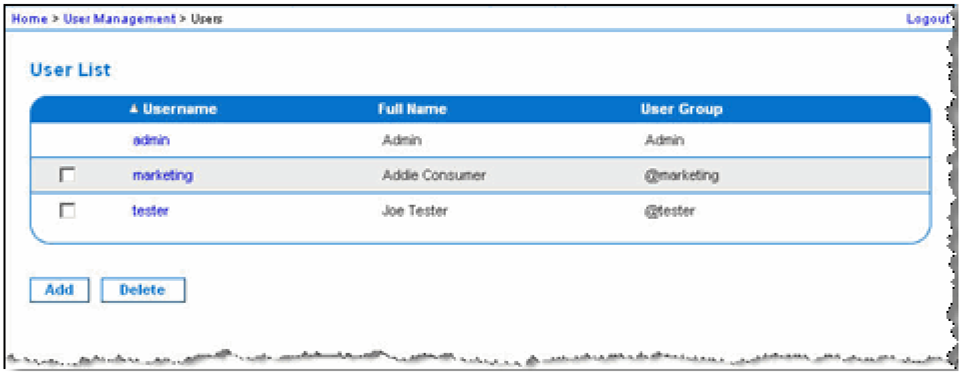
Users must be granted user names and passwords to gain access to the Dominion KX II. This information is used to authenticate users attempting to access your Dominion KX II.

User List

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

➢ *To view the list of users:*

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



	▲ Username	Full Name	User Group
	admin	Admin	Admin
☐	marketing	Addie Consumer	@marketing
☐	tester	Joe Tester	@tester

Adding a New User

It is a good idea to define user groups before creating Dominion KX II users because, when you add a user, you must assign that user to an existing user group. Refer to ***Adding a New User Group*** (on page 198) for more information.

From the User page, you can add new users, modify user information, and reactivate users that have been deactivated.

Note: A user name can be deactivated when the number of failed login attempts has exceeded the maximum login attempts set in the Security Settings page. Refer to ***Security Settings*** (on page 248) for more information.

➢ *To add a new user:*

1. Open the User page by choosing User Management > Add New User or clicking the Add button on the User List page.
2. Type a unique name in the Username field (up to 16 characters).
3. Type the person's full name in the Full Name field (up to 64 characters).

4. Type a password in the Password field and retype the password in the Confirm Password field (up to 64 characters).
5. Choose the group from the User Group drop-down list. The list contains all groups you have created in addition to the system-supplied default groups (<Unknown> (default setting), Admin, Individual Group).

   If you do not want to associate this user with an existing User Group, select Individual Group from the drop-down list. For more information about permissions for an Individual Group, refer to ***Setting Permissions for an Individual Group*** (on page 203).
6. To activate the new user, select the Active checkbox. The default is activated (enabled).
7. Click OK.

Modifying an Existing User

➢ ***To modify an existing user:***

1. Locate the user from among those listed on the User List page.
2. Click the user name. The User page opens.
3. On the User page, change the appropriate fields. (Refer to Adding a New User for information about how to get access the User page.)
4. To delete a user, click Delete. You are prompted to confirm the deletion.
5. Click OK.

Authentication Settings

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

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

From the Authentication Settings page you can configure the type of authentication used for access to your Dominion KX II.

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

➢ *To configure authentication:*

1. Choose User Management > Authentication Settings. The Authentication Settings page opens.
2. Choose the option for the authentication protocol you want to use (Local Authentication, LDAP/LDAPS, or RADIUS). Choosing the LDAP option enables the remaining LDAP fields; selecting the RADIUS option enables the remaining RADIUS fields.
3. If you choose Local Authentication, proceed to step 6.
4. If you choose LDAP/LDAPS, read the section entitled ***Implementing LDAP Remote Authentication*** (see "Implementing LDAP/LDAPS Remote Authentication" on page 211) for information about completing the fields in the LDAP section of the Authentication Settings page.
5. If you choose RADIUS, read the section entitled ***Implementing RADIUS Remote Authentication*** (on page 213) for information about completing the fields in the RADIUS section of the Authentication Settings page.
6. Click OK to save.

➢ *To return to factory defaults:*

- Click the Reset to Defaults button.

User Authentication Settings

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

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

From the Authentication Settings page you can configure the type of authentication used for access to your Dominion KX II.

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

➢ *To configure authentication:*

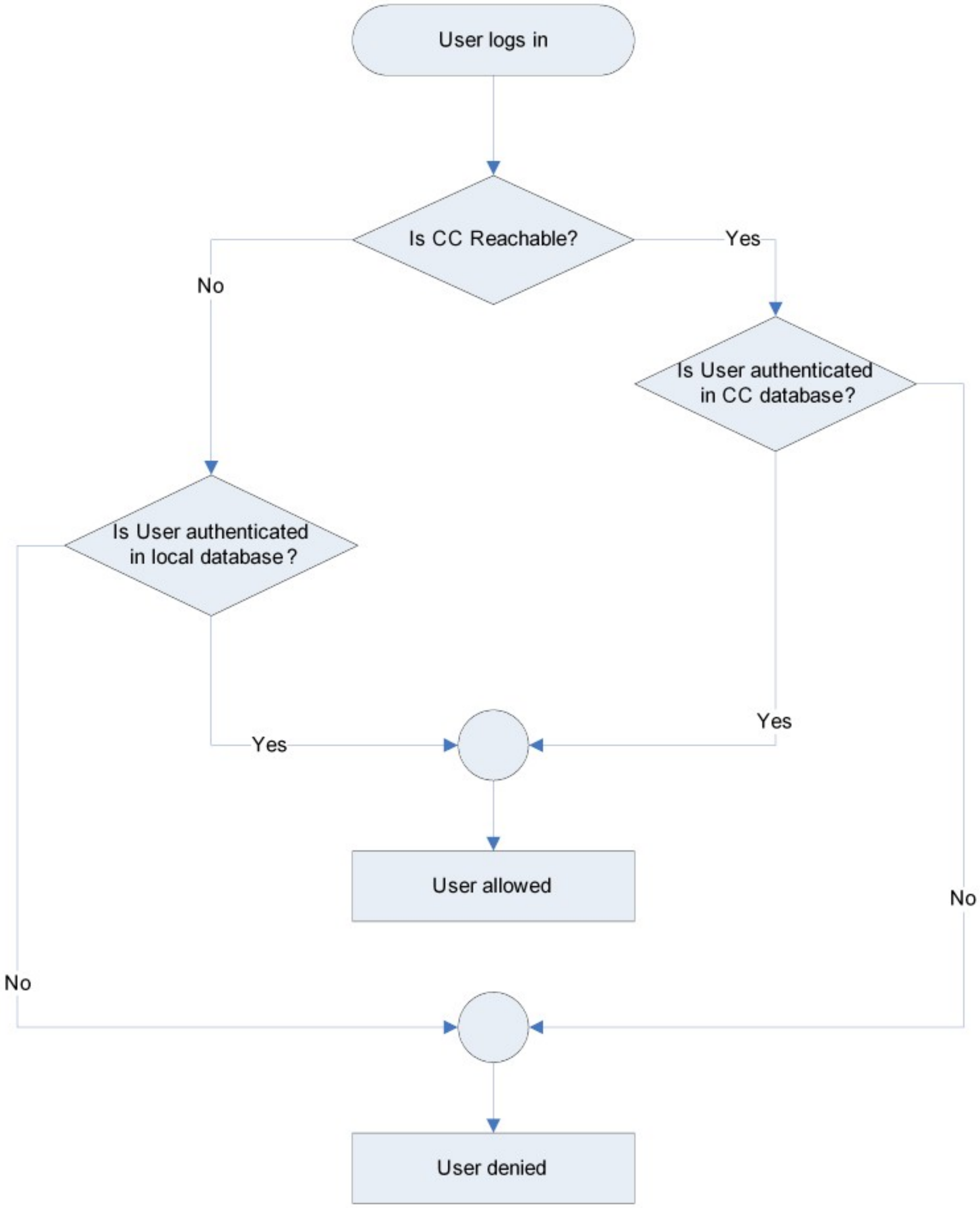
1. Choose User Management > Authentication Settings. The Authentication Settings page opens.
2. Choose the option for the authentication protocol you want to use (Local Authentication, LDAP/LDAPS, or RADIUS). Choosing the LDAP option enables the remaining LDAP fields; selecting the RADIUS option enables the remaining RADIUS fields.
3. If you choose Local Authentication, proceed to step 6.
4. If you choose LDAP/LDAPS, read the section entitled ***Implementing LDAP Remote Authentication*** (see "Implementing LDAP/LDAPS Remote Authentication" on page 211) for information about completing the fields in the LDAP section of the Authentication Settings page.
5. If you choose RADIUS, read the section entitled ***Implementing RADIUS Remote Authentication*** (on page 213) for information about completing the fields in the RADIUS section of the Authentication Settings page.
6. Click OK to save.

➢ *To return to factory defaults:*

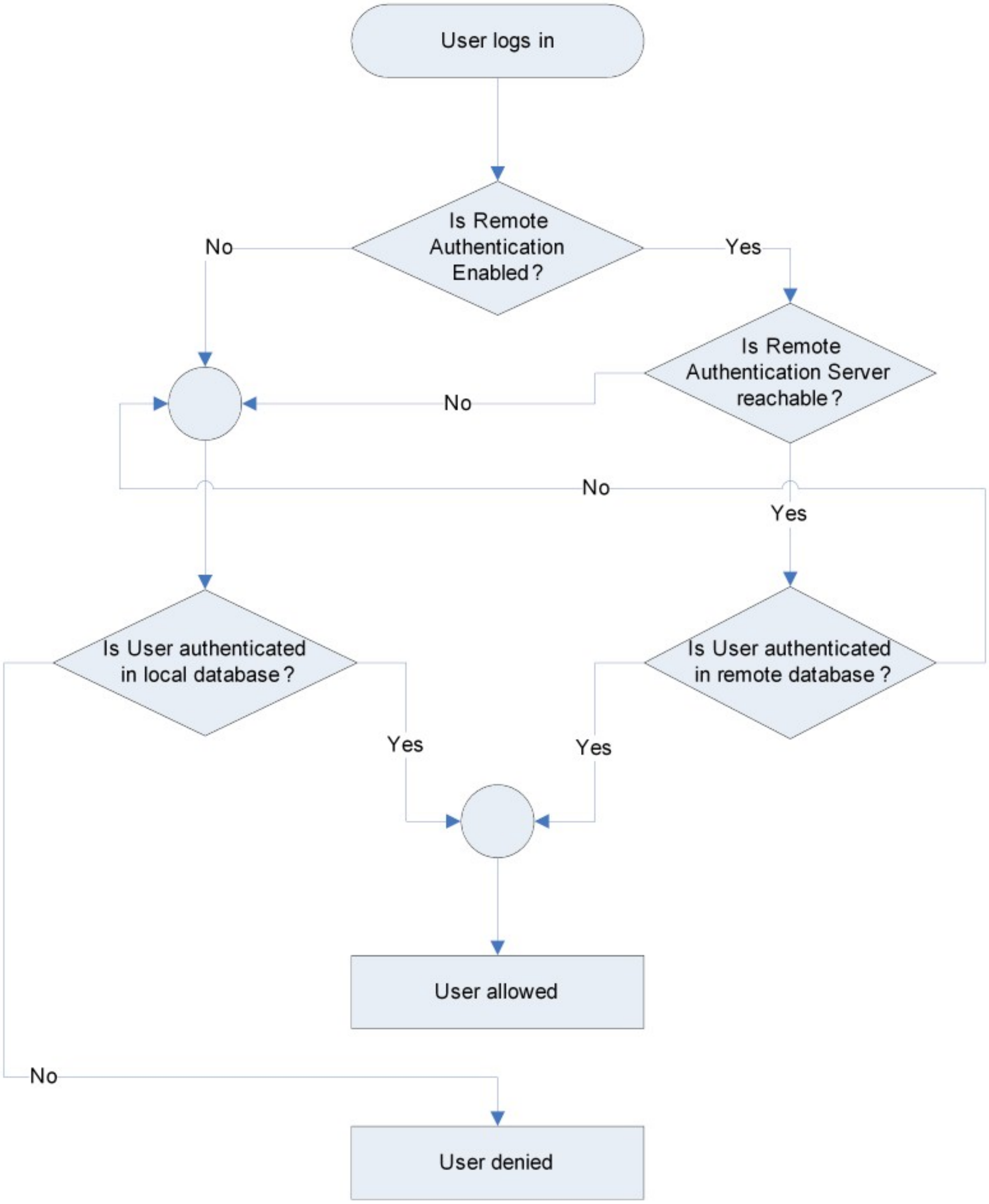
- Click the Reset to Defaults button.

User Authentication Process

When the device is configured to authenticate and authorize local users from CC, the order in which the user credentials are validated follows the following process:


User logs in
Is CC Reachable?
No
Yes
Is User authenticated in CC database?
Is User authenticated in local database?
Yes
Yes
User allowed
No
No
User denied

Remote authentication follows the process specified in the flowchart below:


User logs in
Is Remote Authentication Enabled?
No
Yes
Is Remote Authentication Server reachable?
No
No
Yes
Is User authenticated in local database?
Is User authenticated in remote database?
Yes
Yes
User allowed
No
User denied

Implementing LDAP/LDAPS Remote Authentication

Lightweight Directory Access Protocol (LDAP/LDAPS) is a networking protocol for querying and modifying directory services running over TCP/IP. A client starts an LDAP session by connecting to an LDAP/LDAPS server (the default TCP port is 389). The client then sends operation requests to the server, and the server sends responses in turn.

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

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

1. Click Device > Network to open the Network Settings page.
2. Type the IP address or DNS name of your LDAP/LDAPS remote authentication server in the Primary LDAP Server field. When the Enable Secure LDAP option is selected, the DNS name must be used.
3. Type the IP address or DNS name of your backup LDAP/LDAPS server in the Secondary LDAP Server field. When the Enable Secure LDAP option is selected, the DNS name must be used. Note that the remaining fields share the same settings with the Primary LDAP Server field. **Optional**
4. Type the server secret (password) required to authenticate against your remote authentication server in the Secret Phrase field and again in the Confirm Secret Phrase field. Enter the password in use on the LDAP/LDAPS server.
5. Dialback Query String. Type the dialback query string. If you are using Microsoft Active Directory, you must enter the following string:

   msRADIUSCallbackNumber

   Note: This string is case sensitive.

6. Select the Enable Secure LDAP checkbox if you would like to use SSL; the Secure LDAP Port field is enabled. Secure Sockets Layer (SSL) is a cryptographic protocol that allows Dominion KX II to communicate securely with the LDAP/LDAPS server.
7. The default Port is 389. Either use the standard LDAP TCP port or specify another port.

8. The default Secure LDAP Port is 636. Either use the default port or specify another port. This field is enabled when the Enable Secure LDAP checkbox is selected.
9. Certificate File. Consult your authentication server administrator to get the CA certificate file in Base64 encoded X-509 format for the LDAP/LDAPS server. Use the Browse button to navigate to the certificate file. This field is enabled when the Enable Secure LDAP option is selected.
10. DN of administrative User. Distinguished Name of administrative user; consult your authentication server administrator for the appropriate values to type into this field. An example DN of administrative User value might be: *cn=Administrator,cn=Users,dc=testradius,dc=com*.
11. User Search DN. This describes the name you want to bind against the LDAP/LDAPS, and where in the database to begin searching for the specified Base DN. An example Base Search value might be: *cn=Users,dc=raritan,dc=com*. Consult your authentication server administrator for the appropriate values to enter into these fields.
12. Type of external LDAP/LDAPS server. Choose from among the options available:
    - Generic LDAP Server.
    - Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
13. Active Directory Domain. Type the name of the Active Directory Domain.

Returning User Group Information from Active Directory Server

The Dominion KX II supports user authentication to Active Directory (AD) without requiring that users be defined locally on the Dominion KX II. This allows Active Directory user accounts and passwords to be maintained exclusively on the AD server. Authorization and AD user privileges are controlled and administered through the standard Dominion KX II policies and user group privileges that are applied locally to AD user groups.

IMPORTANT: If you are an existing Raritan, Inc. customer, and have already configured the Active Directory server by changing the AD schema, Dominion KX II still supports this configuration and you do not need to perform the following operations. Refer to *Updating the*

LDAP Schema **(on page 302) for information about updating the AD LDAP/LDAPS schema.**

➢ *To enable your AD server on the Dominion KX II:*

1. Using Dominion KX II, create special groups and assign proper permissions and privileges to these groups. For example, create groups such as KVM_Admin and KVM_Operator.
2. On your Active Directory server, create new groups with the same group names as in the previous step.
3. On your AD server, assign the Dominion KX II users to the groups created in step 2.
4. From the Dominion KX II, enable and configure your AD server properly. Refer to ***Implementing LDAP/LDAPS Remote Authentication*** (on page 211).

Important Notes:

- Group Name is case sensitive.
- The Dominion KX II provides the following default groups that cannot been changed or deleted: Admin and <Unknown>. Verify that your Active Directory server does not use the same group names.
- If the group information returned from the Active Directory server does not match a Dominion KX II group configuration, the Dominion KX II automatically assigns the group of <Unknown> to users who authenticate successfully.
- If you use a dialback number, you must enter the following case-sensitive string: *msRADIUSCallbackNumber*

Implementing RADIUS Remote Authentication

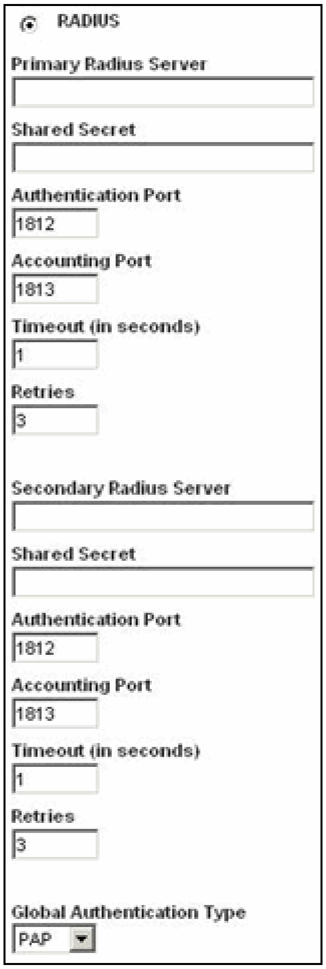
Remote Authentication Dial-in User Service (RADIUS) is an AAA (authentication, authorization, and accounting) protocol for network access applications.

➢ *To use the RADIUS authentication protocol:*

1. Type the IP address of your primary and optional secondary remote authentication servers in the Primary Radius Server and Secondary Radius Server fields, respectively.

2. Type the server secret used for authentication (in the Shared Secret fields). The shared secret is a character string that must be known by both the Dominion KX II and the RADIUS server to allow them to communicate securely. It is essentially a password.
3. Authentication Port. The default authentication port is 1812; change as required.
4. Accounting Port. The default accounting port is 1813; change as required.
5. Timeout (in seconds). The default timeout is 1 second; change as required. The timeout is the length of time the Dominion KX II waits for a response from the RADIUS server before sending another authentication request.
6. Retries. The default number of retries is 3; change as required. This is the number of times the Dominion KX II will send an authentication request to the RADIUS server.
7. Global Authentication Type. Choose from among the options in the drop-down list:
   - PAP - With PAP, passwords are sent as plain text. PAP is not interactive; the user name and password are sent as one data package once a connection is established, rather than the server sending a login prompt and waiting for a response.

- CHAP - With CHAP, authentication can be requested by the server at any time. CHAP provides more security than PAP.



● RADIUS

Primary Radius Server

Shared Secret

Authentication Port
1812

Accounting Port
1813

Timeout (in seconds)
1

Retries
3

Secondary Radius Server

Shared Secret

Authentication Port
1812

Accounting Port
1813

Timeout (in seconds)
1

Retries
3

Global Authentication Type
PAP

Returning User Group Information via RADIUS

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

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

Raritan:G{GROUP_NAME}

where GROUP_NAME is a string, denoting the name of the group to which the user belongs.

Raritan:G{GROUP_NAME}:D{Dial Back Number}

where GROUP_NAME is a string denoting the name of the group to which the user belongs and Dial Back Number is the number associated with the user account that the Dominion KX II modem will use to dial back to the user account.

RADIUS Communication Exchange Specifications

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

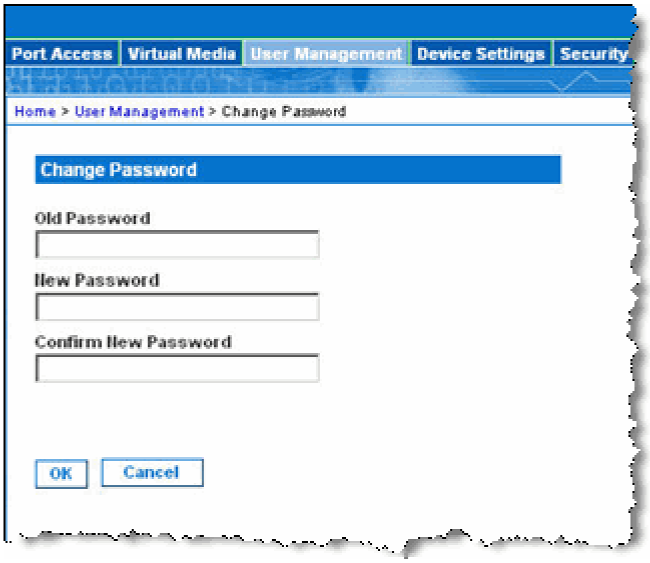
Attribute	Data
Log on	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-IP-Address (4)	The IP address for the Dominion KX II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
User-Password(2)	The encrypted password.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

Attribute	Data
Log on	
NAS-IP-Address (4)	The IP address for the Dominion KX II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
Log off	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - Stops the accounting
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP address for the Dominion KX II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

Change a Password

➤ ***To change your password:***

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



2. Type your current password in the Old Password field.

3. Type a new password in the New Password field; retype the new password in the Confirm New Password field. Passwords can be up to 64 characters in length and can consist of English alphanumeric characters and special characters.

4. Click OK.

5. You will receive confirmation that the password was successfully changed. Click OK.

Note: If strong passwords are in use, this page displays information about the format required for the passwords. For more information about passwords and strong passwords, refer to ***Strong Passwords*** (on page 250).

Chapter 7 Device Management

In This Chapter

Network Settings

Use the Network Settings page to customize the network configuration (for example, the IP address, discovery port, and LAN interface parameters) for your Dominion KX II unit.

Important: The Dominion KX II must be rebooted for new network settings to take effect. Before changing the network configuration, ensure that there are no other active user connections to the device. All connections will be dropped when the Dominion KX II unit reboots.

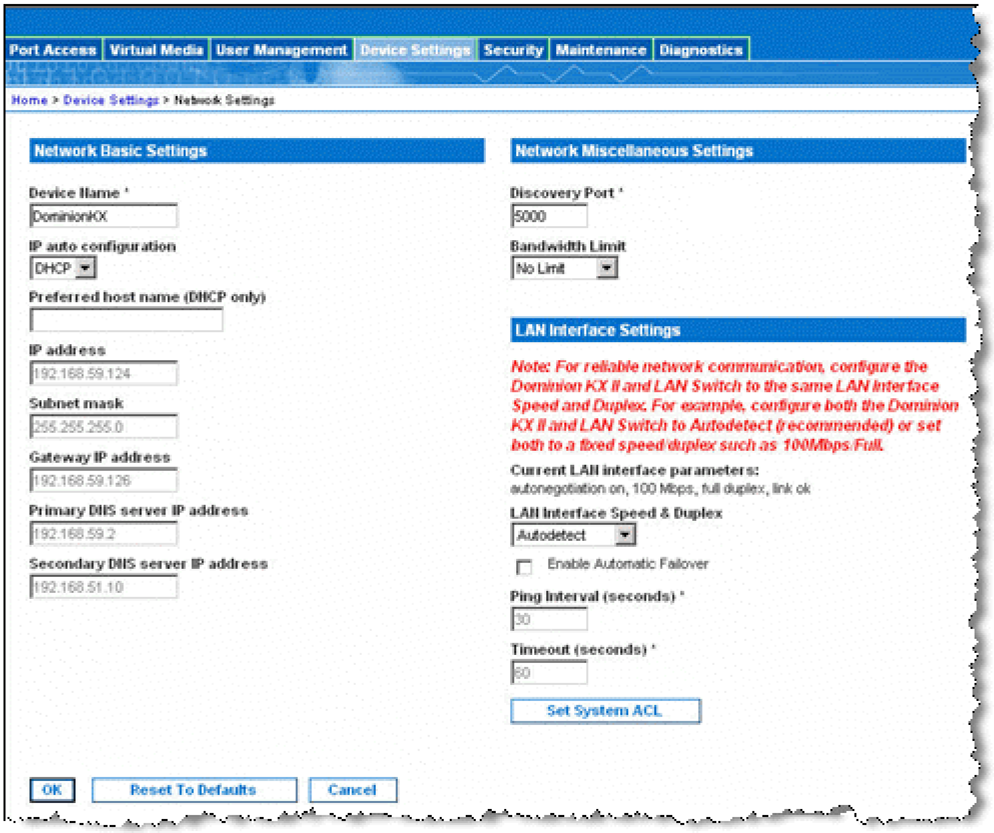
Basically, there are two options available to setup your IP configuration:

- None (default) - This is the recommended option (static IP). Since the Dominion KX II is part of your network infrastructure, you most likely do not want its IP address to change frequently. This option allows you to set the network parameters.
- DHCP - With this option the IP address is automatically assigned by a DHCP server.

➢ ***To change the network configuration:***

1. Choose Device Settings > Network. The Network Settings page opens.
2. Update the Network Basic Settings. Refer to ***Network Basic Settings*** (on page 220) for more information about each of the fields.
3. Update the Network Miscellaneous Settings. Refer to ***Network Miscellaneous Settings*** (on page 222) for more information about each of the fields.
4. Update the LAN Interface Settings. Refer to ***LAN Interface Settings*** (on page 222) for more information about each of the fields.

5. Click OK to set these configurations. If your changes require rebooting the device, a reboot message appears.



Network Basic Settings

Device Name * DominionKX

IP auto configuration DHCP

Preferred host name (DHCP only)

IP address 192.168.59.124

Subnet mask 255.255.255.0

Gateway IP address 192.168.59.126

Primary DNS server IP address 192.168.59.2

Secondary DNS server IP address 192.168.51.10

Network Miscellaneous Settings

Discovery Port * 5000

Bandwidth Limit No Limit

LAN Interface Settings

Note: For reliable network communication, configure the Dominion KX II and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX II and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.

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

LAN Interface Speed & Duplex Autodetect

□ Enable Automatic Failover

Ping Interval (seconds) * 30

Timeout (seconds) * 60

➢ ***To reset to factory defaults:***

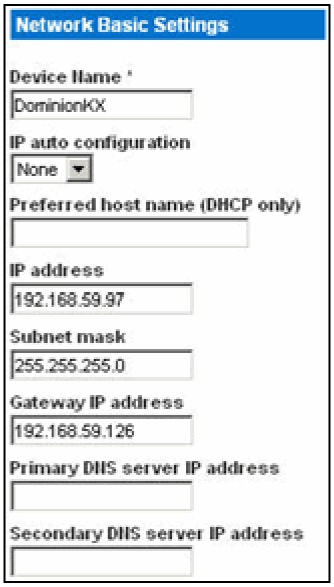
- Click Reset to Defaults.

Network Basic Settings

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

If None is selected for the IP auto configuration, the following Network Basic Settings fields are enabled, allowing you to manually set the IP configuration.

  - IP Address - The default IP address is 192.168.0.192.
  - Subnet Mask - The default subnet mask is 255.255.255.0.
  - Gateway IP Address - The IP address for the gateway (if one is used).
  - Primary DNS Server IP Address - The primary Domain Name Server used to translate names into IP addresses.
  - Secondary DNS Server IP Address - The secondary Domain Name Server used to translate names into IP addresses (if one is used).
- DHCP - Dynamic Host Configuration Protocol is used by networked computers (clients) to obtain unique IP addresses and other parameters from a DHCP server. If DHCP is used, enter the Preferred host name (DHCP only). Up to 63 characters.



Network Basic Settings

Device Name *
DominionKX

IP auto configuration
None

Preferred host name (DHCP only)

IP address
192.168.59.97

Subnet mask
255.255.255.0

Gateway IP address
192.168.59.126

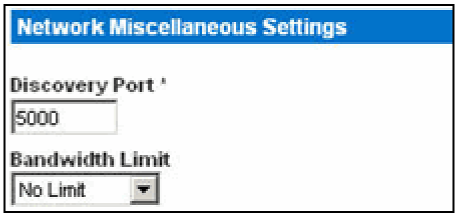
Primary DNS server IP address

Secondary DNS server IP address

Network Miscellaneous Settings

- Discovery Port - The Dominion KX II discovery occurs over a single, configurable TCP port. The default is Port 5000, but you can configure it to use any TCP port not in use. To access the Dominion KX II device from beyond a firewall, your firewall settings must enable two-way communication through the default Port 5000 or a nondefault port that you have configured. For more information, refer to ***Step 5: Configure Network Firewall Settings*** (on page 35).
- Bandwidth Limit - The default is No Limit. Choose from among the options in the drop-down list to set a maximum amount of bandwidth that can be consumed by the Dominion KX II device (for all sessions). The options include: No Limit, 100 Megabit, 10 Megabit, 5 Megabit, 2 Megabit, 512 Kilobit, 256 Kilobit, and 128 Kilobit.

Note: Lower bandwidth may result in slower performance.



Network Miscellaneous Settings

Discovery Port *

5000

Bandwidth Limit

No Limit

LAN Interface Settings

- The current parameter settings are identified in the Current LAN interface parameters field.
- LAN Interface Speed & Duplex - Choose from among the speed and duplex combinations available.
  - Autodetect (default option)
  - 10 Mbps/Half - Both LEDs blink
  - 10 Mbps/Full - Both LEDs blink
  - 100 Mbps/Half - Yellow LED blinks
  - 100 Mbps/Full - Yellow LED blinks
  - 1000 Mbps/Full (gigabit) - Green LED blinks
  - Half-duplex provides for communication in both directions, but only one direction at a time (not simultaneously).
  - Full-duplex allows communication in both directions simultaneously.

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

Refer to ***Network Speed Settings*** (on page 300) for more information.

- Enable Automatic Failover - Check this checkbox to allow the Dominion KX II to automatically recover its network connection using a second network port if the active network port fails.

Note: Because a failover port is not activated until after a failover has actually occurred, Raritan recommends that you either not monitor the port or monitor it only after a failover occurs.

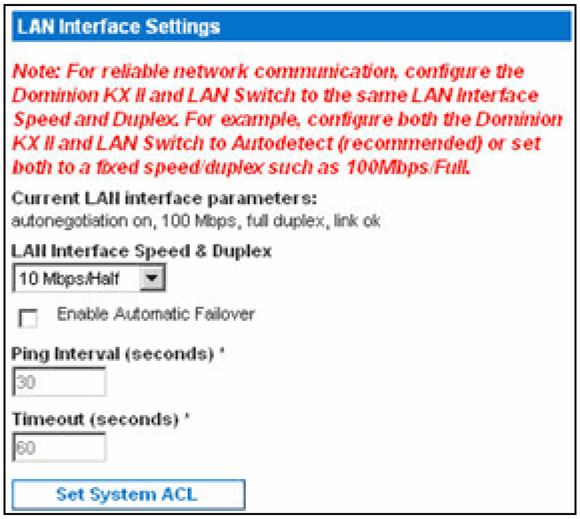
When this option is enabled, the following two fields are used:

- Ping Interval (seconds) - Ping interval determines how often the Dominion KX II checks the status of the network connection (setting this too low may cause excess network traffic). The default ping interval is 30 seconds.
- Timeout (seconds) - Timeout determines how long a network port must be “dead” before the switch is made. Both network ports must be connected to the network. This option must be checked in order for the Automatic Failover to function. The default timeout is 60 seconds.

Note: The default ping interval and timeout causes remote sessions to be dropped when the Dominion KX II device tries to switch over. When this occurs, the remote session needs to be reestablished. Reducing these intervals to much lower values will allow remote sessions to stay connected, but will result in increased network traffic.

- Set System ACL - Click this button to set a global-level Access Control List for your Dominion KX II by ensuring that your device does not respond to packets being sent from disallowed IP addresses. The IP Access Control page opens.

Note: These ACL values are global, affecting the Dominion KX II unit as a whole. You can also create ACLs on a group-level basis. For example, you can create an "Outsourced Vendors" user group that is permitted to access the Dominion KX II only from a given IP address range (refer to ***Group-based IP ACL*** (see "Group-Based IP ACL (Access Control List)" on page 201) for more information on how to create group-specific Access Control Lists).



LAN Interface Settings

Note: For reliable network communication, configure the Dominion KX II and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX II and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.

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

LAN Interface Speed & Duplex
10 Mbps/Half

□ Enable Automatic Failover

Ping Interval (seconds) *
30

Timeout (seconds) *
60

Date/Time Settings

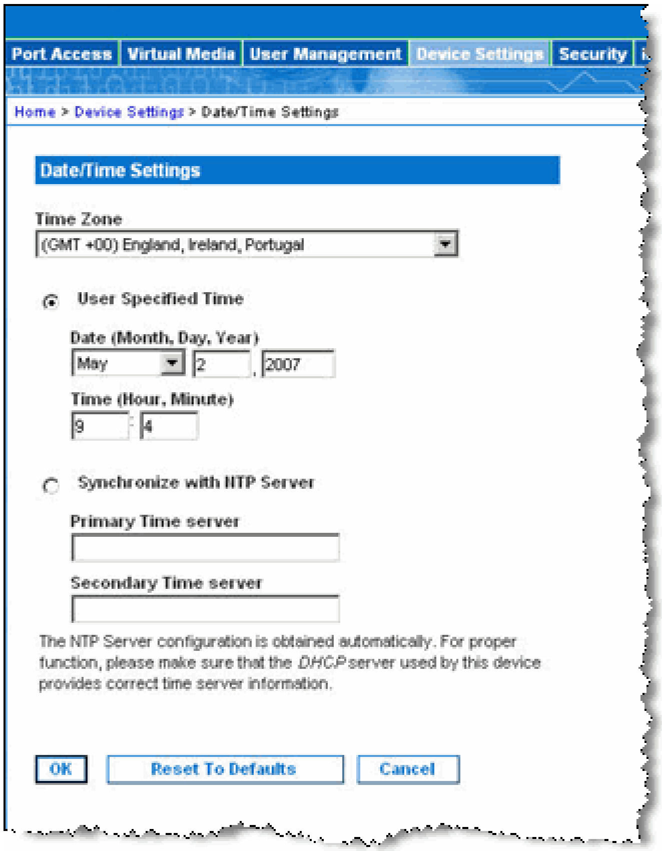
Use the Date/Time Settings page to specify the date and time for the Dominion KX II. There are two ways to do this:

- Manually set the date and time or synchronize with a Network Time Protocol (NTP) server.

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

➢ *To set the date and time:*

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



Date/Time Settings

Time Zone
(GMT +00) England, Ireland, Portugal

● User Specified Time

Date (Month, Day, Year)
May 2 , 2007

Time (Hour, Minute)
9 : 4

○ Synchronize with NTP Server

Primary Time server

Secondary Time server

The NTP Server configuration is obtained automatically. For proper function, please make sure that the *DHCP* server used by this device provides correct time server information.

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

- Synchronize with NTP Server. Choose this option to synchronize the date and time with the Network Time Protocol (NTP) Server.

a. For the User Specified Time option, enter the date and time. For the time, use the hh:mm format (using a 24-hour clock).

4. For the Synchronize with NTP Server option:

   a. Enter the IP address of the Primary Time server.

   b. Enter the IP address of the Secondary Time server. **Optional**

5. Click OK.

Event Management

The Dominion KX II Event Management feature provides a set of screens for enabling and disabling the distribution of system events to SNMP Managers, Syslog, and the audit log. These events are categorized, and for each event you can determine whether you want the event sent to one or several destinations.

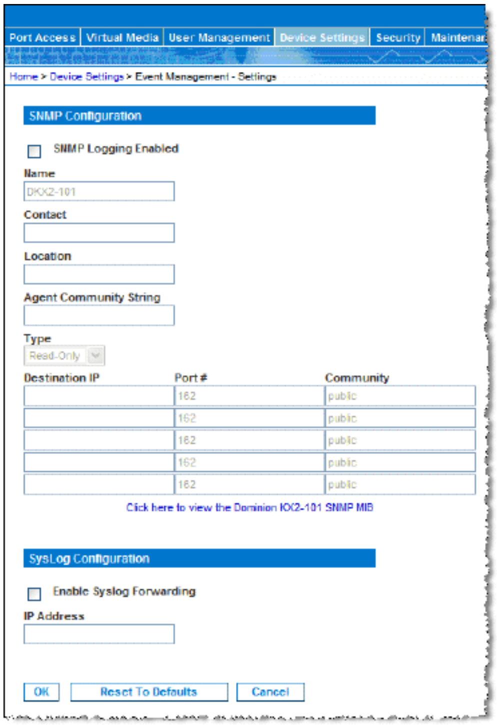
Event Management - Settings

SNMP Configuration

Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions. Dominion KX II offers SNMP Agent support through Event Management.

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

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



SNMP Configuration

□ SNMP Logging Enabled

Name
DKX2-101

Contact

Location

Agent Community String

Type
Read-Only

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

Click here to view the Dominion KX2-101 SNMP MIB

SysLog Configuration

□ Enable Syslog Forwarding

IP Address

2. Choose the Enable SNMP Logging option. This enables the remaining SNMP fields.

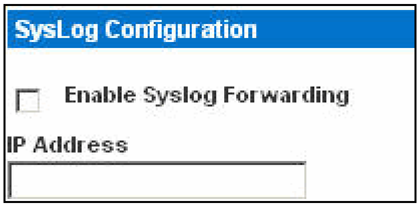
3. In the Name, Contact, and Location fields, type the SNMP agent's name (that is, the device's name) as it appears in the Dominion KX II Console interface, a contact name related to this device, and where the Dominion device is physically located, respectively.

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

Syslog Configuration

➢ ***To configure the Syslog (enable Syslog forwarding):***

1. Choose the Enable Syslog Forwarding option to log the device's messages to a remote Syslog server.
2. Type the IP Address of your Syslog server in the IP Address field.
3. Click OK.



SysLog Configuration

□ Enable Syslog Forwarding

IP Address

➢ ***To reset to factory defaults:***

- Click the Reset To Defaults button.

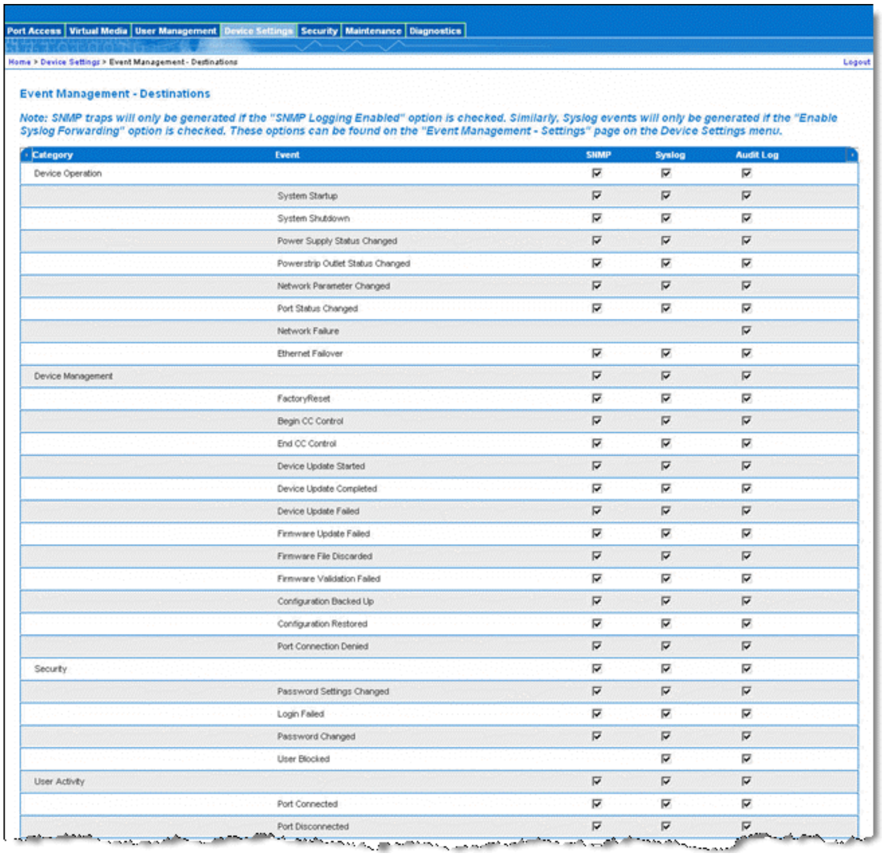
Event Management - Destinations

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

Note: SNMP traps will only be generated if the SNMP Logging Enabled option is selected; Syslog events will only be generated if the Enable Syslog Forwarding option is selected. Both of these options are in the *Event Management - Settings* (on page 227) page.

➢ *To select events and their destinations:*

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



Event Management - Destinations

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

Category	Event	SNMP	Syslog	Audit Log
Device Operation		☑	☑	☑
	System Startup	☑	☑	☑
	System Shutdown	☑	☑	☑
	Power Supply Status Changed	☑	☑	☑
	Powerstrip Outlet Status Changed	☑	☑	☑
	Network Parameter Changed	☑	☑	☑
	Port Status Changed	☑	☑	☑
	Network Failure			☑
	Ethernet Failover	☑	☑	☑
Device Management		☑	☑	☑
	FactoryReset	☑	☑	☑
	Begin CC Control	☑	☑	☑
	End CC Control	☑	☑	☑
	Device Update Started	☑	☑	☑
	Device Update Completed	☑	☑	☑
	Device Update Failed	☑	☑	☑
	Firmware Update Failed	☑	☑	☑
	Firmware File Discarded	☑	☑	☑
	Firmware Validation Failed	☑	☑	☑
	Configuration Backed Up	☑	☑	☑
	Configuration Restored	☑	☑	☑
	Port Connection Denied	☑	☑	☑
Security		☑	☑	☑
	Password Settings Changed	☑	☑	☑
	Login Failed	☑	☑	☑
	Password Changed	☑	☑	☑
	User Blocked		☑	☑
User Activity		☑	☑	☑
	Port Connected	☑	☑	☑
	Port Disconnected	☑	☑	☑

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

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

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

3. Click OK.

➢ ***To reset to factory defaults:***

- Click the Reset To Defaults button.

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

SNMP Agent Configuration

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

SNMP Trap Configuration

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

Trap Name	Description
configBackup	The device configuration has been backed up.
configRestore	The device configuration has been restored.
deviceUpdateFailed	Device update has failed.
deviceUpgradeCompleted	The Dominion KX II has completed update via an RFP file.
deviceUpgradeStarted	The Dominion KX II has begun update via an RFP file.
factoryReset	The device has been reset to factory defaults.
firmwareFileDiscarded	Firmware file was discarded.
firmwareUpdateFailed	Firmware update failed.
firmwareValidationFailed	Firmware validation failed.

Trap Name	Description
groupAdded	A group has been added to the Dominion KX II system.
groupDeleted	A group has been deleted from the system.
groupModified	A group has been modified.
ipConflictDetected	An IP Address conflict was detected.
ipConflictResolved	An IP Address conflict was resolved.
networkFailure	An Ethernet interface of the product can no longer communicate over the network.
networkParameterChanged	A change has been made to the network parameters.
passwordSettingsChanged	Strong password settings have changed.
portConnect	A previously authenticated user has begun a KVM session.
portConnectionDenied	A connection to the target port was denied.
portDisconnect	A user engaging in a KVM session closes the session properly.
portStatusChange	The port has become unavailable.
powerNotification	The power outlet status notification: 1=Active, 0=Inactive.
powerOutletNotification	Power strip device outlet status notification.
rebootCompleted	The Dominion KX II has completed its reboot.
rebootStarted	The Dominion KX II has begun to reboot, either through cycling power to the system or by a warm reboot from the OS.
securityViolation	Security violation.
startCCManagement	The device has been put under CommandCenter Management.
stopCCManagement	The device has been removed from CommandCenter Management.
userAdded	A user has been added to the system.
userAuthenticationFailure	A user attempted to log in without a correct username and/or password.

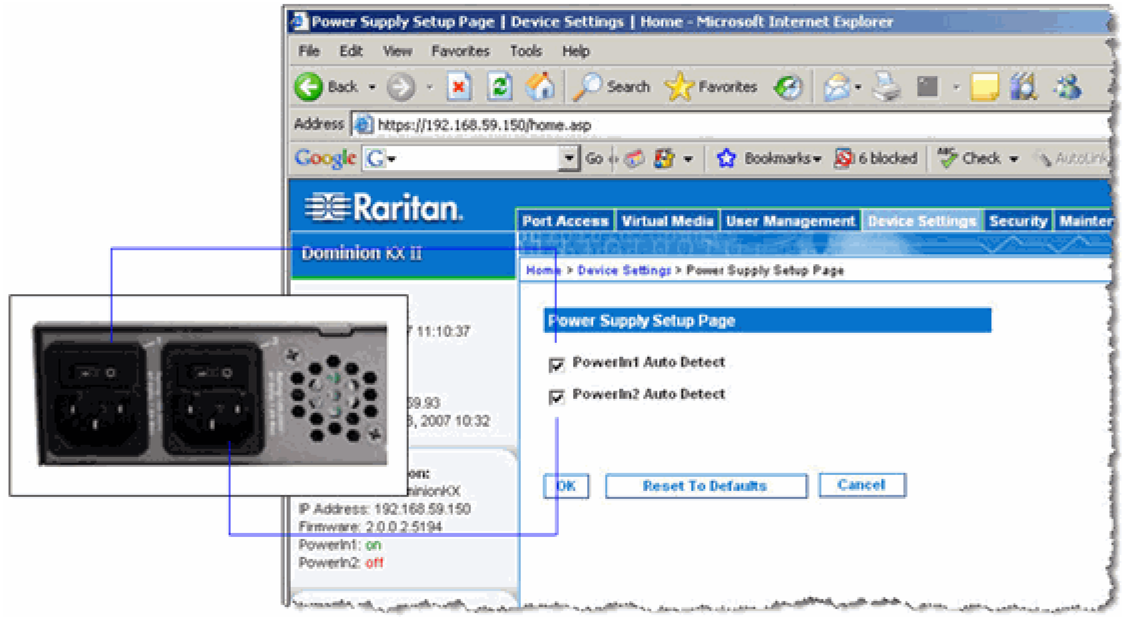
Trap Name	Description
userConnectionLost	A user with an active session has experienced an abnormal session termination.
userDeleted	A user account has been deleted.
userLogin	A user has successfully logged into the Dominion KX II and has been authenticated.
userLogout	A user has successfully logged out of the Dominion KX II properly.
userModified	A user account has been modified.
userPasswordChanged	This event is triggered if the password of any user of the device is modified.
userSessionTimeout	A user with an active session has experienced a session termination due to timeout.
vmImageConnected	User attempted to mount either a device or image on the target using Virtual Media. For every attempt on device/image mapping (mounting) this event is generated.
vmImageDisconnected	User attempted to unmount a device or image on the target using Virtual Media.

Power Supply Setup Page

The Dominion KX II provides dual power supplies, and can automatically detect and provide notification regarding the status of these power supplies. Use the Power Supply Setup page to specify whether you are using one or both of the power supplies. Proper configuration ensures that the Dominion KX II sends the appropriate notifications should a power supply fail. For example, if power supply number one fails, the power LED at the front of the unit will turn red.

➤ ***To enable automatic detection for the power supplies in use:***

1. Choose Device Settings > Power Supply Setup. The Power Supply Setup page opens.



Power Supply Setup Page | Device Settings | Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.59.150/home.asp
Google Go Bookmarks 6 blocked Check AutoLink
Raritan.
Dominion KX II
Port Access Virtual Media User Management Device Settings Security Mainter
Home > Device Settings > Power Supply Setup Page

Power Supply Setup Page

☑ PowerIn1 Auto Detect

☑ PowerIn2 Auto Detect

OK | Reset To Defaults | Cancel

IP Address: 192.168.59.150
Firmware: 2.0.0.2.5194
PowerIn1: on
PowerIn2: off

2. If you are plugging power input into power supply number one (left-most power supply at the back of the unit), then select the Powerln1 Auto Detect option.

3. If you are plugging power input into power supply number two (right-most power supply at the back of the unit), then select the Powerln2 Auto Detect option.

4. Click OK.

Note: If either of these checkboxes is selected and power input is not actually connected, the power LED at the front of the unit turns red.

➢ *To turn off the automatic detection:*

Deselect the checkbox for the appropriate power supply.

➢ *To reset to factory defaults:*

- Click the Reset To Defaults button.

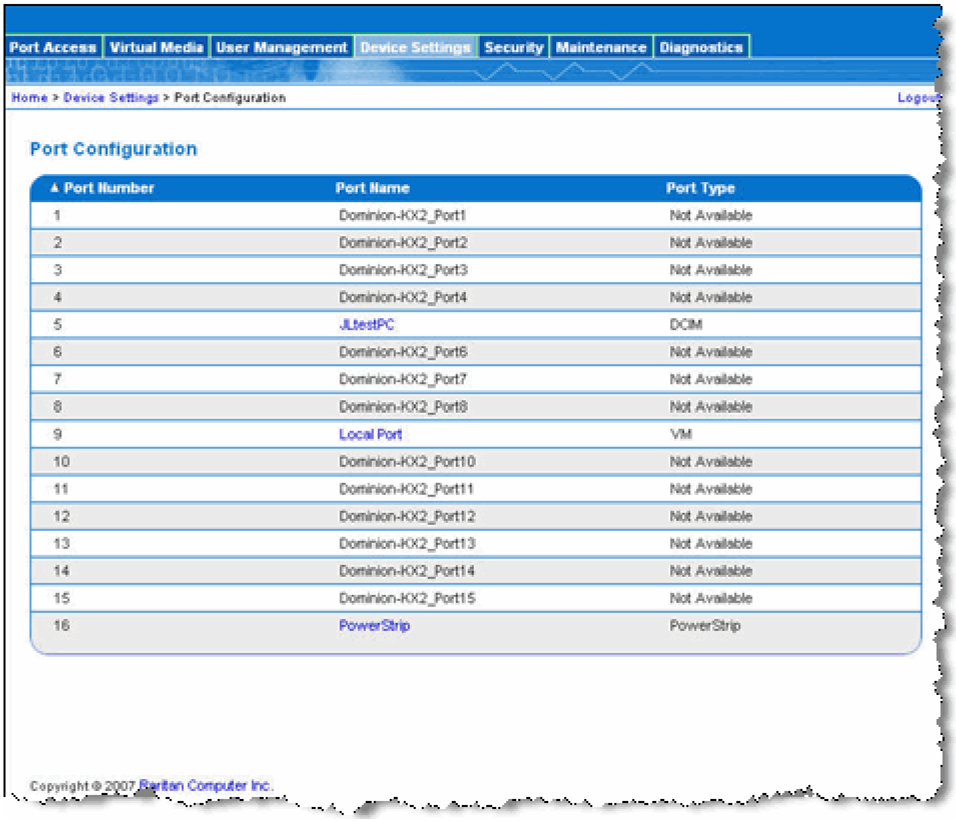
Note: The Dominion KX II does NOT report power supply status to CommandCenter. Dominion I (generation 1), however, does report power supply status to CommandCenter.

Port Configuration Page

The Port Configuration page displays a list of the Dominion KX II ports. Ports connected to KVM target servers or power strips are displayed in blue and can be edited. For ports with no CIM connected or with a blank CIM name, a default port name of Dominion-KX2_Port# is assigned, where Port# is the number of the Dominion KX II physical port.

➢ ***To change a port configuration:***

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



Home > Device Settings > Port Configuration

Port Configuration

▲ Port Number	Port Name	Port Type
1	Dominion-KX2_Port1	Not Available
2	Dominion-KX2_Port2	Not Available
3	Dominion-KX2_Port3	Not Available
4	Dominion-KX2_Port4	Not Available
5	JLtestPC	DCIM
6	Dominion-KX2_Port6	Not Available
7	Dominion-KX2_Port7	Not Available
8	Dominion-KX2_Port8	Not Available
9	Local Port	VM
10	Dominion-KX2_Port10	Not Available
11	Dominion-KX2_Port11	Not Available
12	Dominion-KX2_Port12	Not Available
13	Dominion-KX2_Port13	Not Available
14	Dominion-KX2_Port14	Not Available
15	Dominion-KX2_Port15	Not Available
16	PowerStrip	PowerStrip

Copyright © 2007 Raritan Computer Inc.

This page is initially displayed in port number order, but can be sorted on any of the fields by clicking on the column heading.

- Port Number - Numbered from 1 to the total number of ports available for the Dominion KX II device.
- Port Name - The name assigned to the port. A port name displayed in black indicates that you cannot change the name and that the port cannot be edited; port names displayed in blue can be edited.

Note: Do not use apostrophes for the Port (CIM) Name.

- Port Type - The type of CIM connected to the port:

Port type	Description
DCIM	Dominion CIM
Not Available	No CIM connected
PCIM	Paragon CIM
PowerStrip	Power CIM
VM	Virtual Media CIM (D2CIM-VUSB and D2CIM-DVUSB)

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

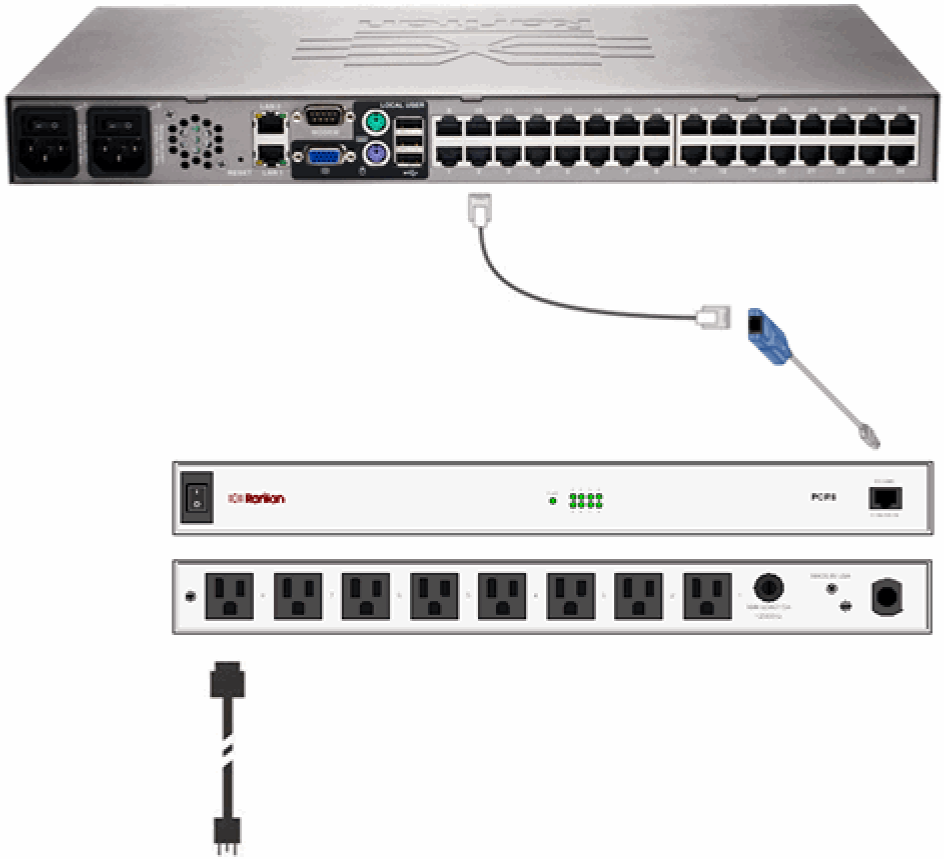
Power Control

Connect the Power Strip

➢ ***To connect the power strip:***

1. Connect the male RJ-45 of the D2CIM-PWR to the female RJ-45 connector on the power strip.
2. Connect the female RJ-45 connector of the D2CIM-PWR to any of the available female system port connectors on the Dominion KX II using a straight through Cat 5 cable.
3. Attach an AC power cord to the target server and an available power strip outlet.
4. Connect the power strip to an AC power source.

5. Power on the Dominion KX II unit.



Name the Power Strip (Port Page for Power Strips)

This Port page opens when you select a port from the Port Configuration page that is connected to a Raritan remote power strip. The Type and the Name fields are prepopulated; note that the (CIM) Type cannot be changed. The following information is displayed for each outlet in the power strip: [Outlet] Number, Name, and Port Association.

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

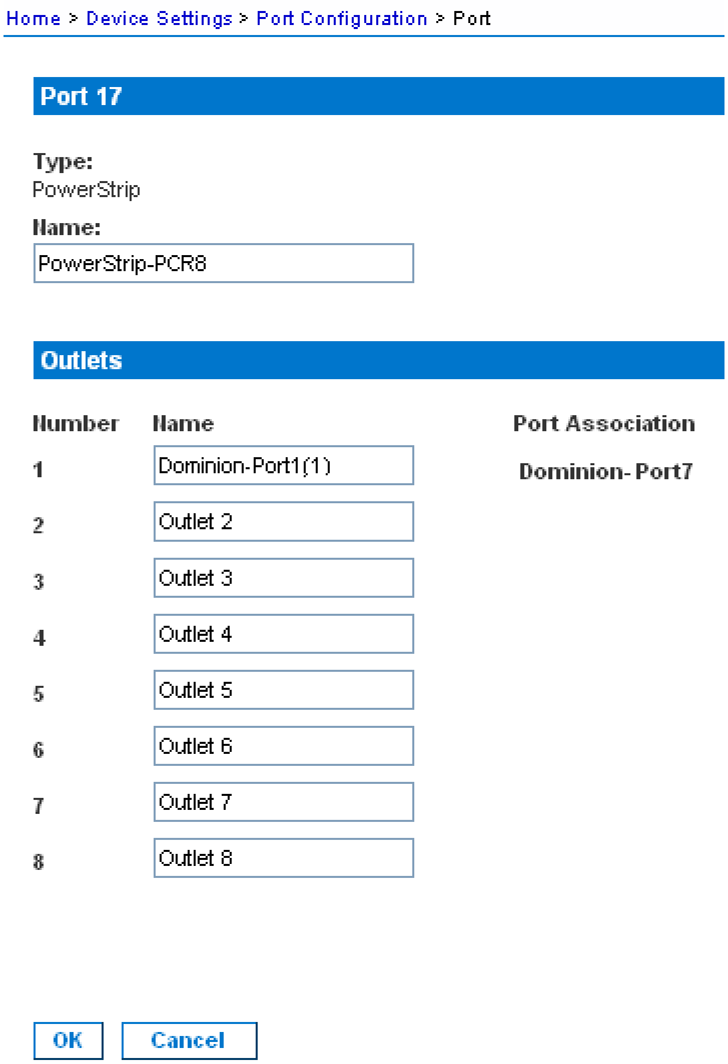
Note: When a power strip is associated with a target server (port), the outlet name is replaced by the target server name (even if you assigned another name to the outlet).

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

Note: CommandCenter Service Gateway does not recognize power strip names containing spaces.

1. Change the Name of the power strip to something you will remember.
2. Change the [Outlet] Name if desired. (Outlet names default to the outlet #.)

3. Click OK.



Port 17

Type:
PowerStrip

Name:
PowerStrip-PCR8

Outlets

Number	Name	Port Association
1	Dominion-Port1(1)	Dominion- Port7
2	Outlet 2	
3	Outlet 3	
4	Outlet 4	
5	Outlet 5	
6	Outlet 6	
7	Outlet 7	
8	Outlet 8	

Associate KVM Target Servers to Outlets (Port Page)

This Port page opens when you select a port from the Port Configuration page that is connected to a target server. From this page, you can make power associations, change the port name to something more descriptive, and update target server settings if you are using the D2CIM-VUSB CIM. The (CIM) Type and the (Port) Name fields are prepopulated; note that the CIM type cannot be changed.

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

To use this feature, you will need:

- Raritan remote power strip(s)
- Power CIMs (D2CIM-PWR)

➢ ***To make power associations (associate power strip outlets to KVM target servers):***

Note: When a power strip is associated to a target server (port), the outlet name is replaced by the target server name (even if you assigned another name to the outlet).

1. Choose the power strip from the Power Strip Name drop-down list.
2. For that power strip, choose the outlet from the Outlet Name drop-down list.
3. Repeat steps 1 and 2 for all desired power associations.
4. Click OK. A confirmation message is displayed.

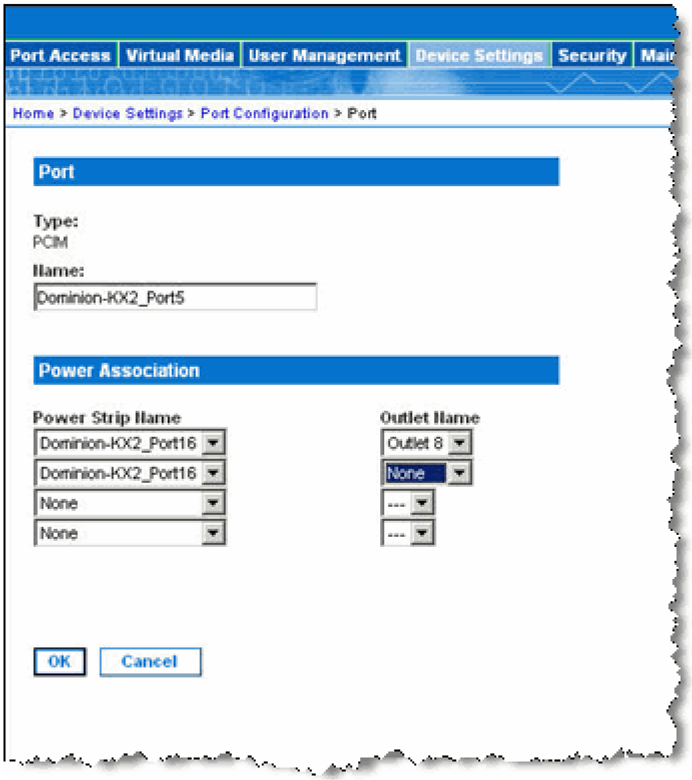
➢ ***To change the port name:***

1. Type something descriptive in the Name field. For example, the name of the target server would be a likely candidate. The name can be up to 32 alphanumeric characters and can include special characters.
2. Click OK.

➢ ***To remove a power strip association:***

1. Select the appropriate power strip from the Power Strip Name drop-down list.

2. For that power strip, select the appropriate outlet from the Outlet Name drop-down list.
3. From the Outlet Name drop-down list, select None.
4. Click OK. That power strip/outlet association is removed and a confirmation message is displayed.



Port

Type:
PCIM

Name:
Dominion-KX2_Port5

Power Association

Power Strip Name	Outlet Name
Dominion-KX2_Port16	Outlet 8
Dominion-KX2_Port16	None
None	---
None	---

Note for D2CIM-VUSB CIM Usage

If you are using the D2CIM-VUSB, there are additional settings on the Port page used to improve performance. Specifically:

- If you are experiencing synchronization issues and are using the D2CIM-VUSB CIM for a Mac target server, check the "Absolute mouse scaling for MAC server" option.
- Certain BIOS do not support USB high-speed capabilities and the attempt to autonegotiate does not work. If you are experiencing BIOS problems with the target server, check the Use Full Speed for Virtual Media CIM option.

Note: For SUSE 9.2 KVM target servers, enable (check) the Use Full Speed for Virtual Media CIM option for those target server ports. SUSE 9.2 does not work with the Virtual Media CIM when high speed is negotiated.

USB Profiles (Port Page)

You choose the available USB profiles for a port in the Select USB Profiles for Port section of the Port page. The USB profiles chosen in the Port page become the profiles available to the user in VKC when connecting to a KVM target server from the port. The default is the Windows 2000/XP/Vista profile. For information about USB profiles, see ***Configuring USB Profiles*** (on page 185).

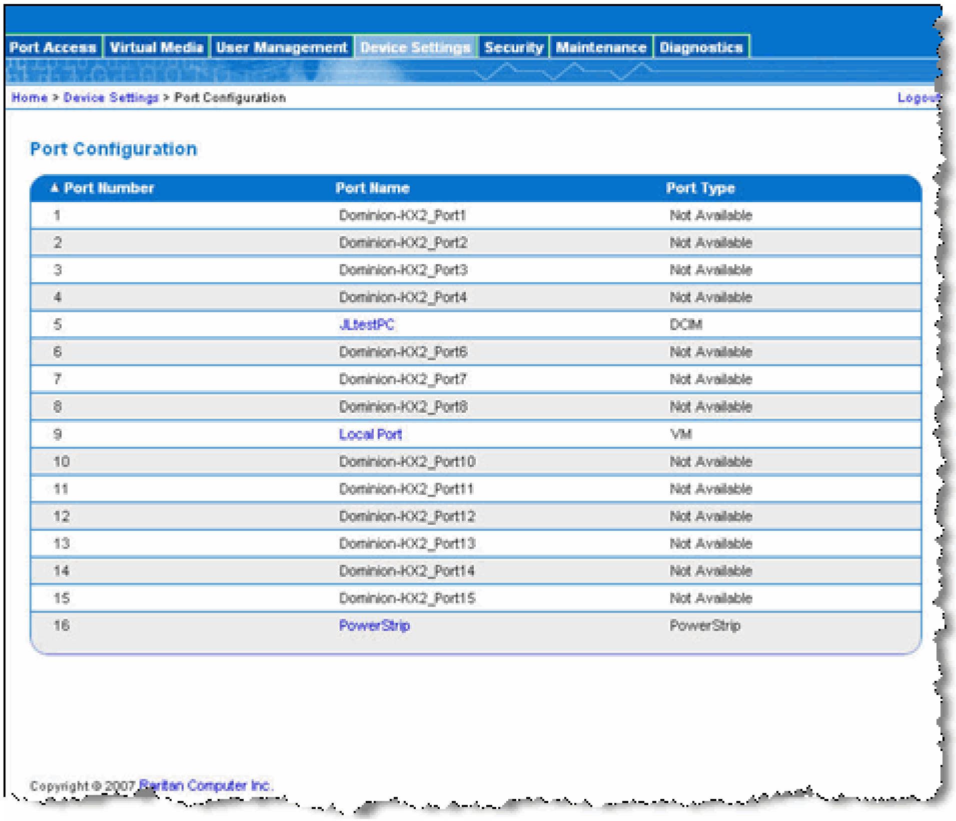
Note: To set USB profiles for a port, you must have a VM-CIM connected with firmware compatible with the current firmware version of the Dominion KX II. See ***Upgrading CIMs*** (on page 264).

The profiles available to assign to a port appear in the Available list on the left. The profiles selected for use with a port appear in the Selected list on the right. When you select a profile in either list, a description of the profile and it's use appears in the Profile Description field.

In addition to selecting a set of profiles to make available for a KVM port, you can also specify the preferred profile for the port and apply the settings set for one port other KVM ports.

➢ *To open the Port page:*

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.



Port Configuration

▲ Port Number	Port Name	Port Type
1	Dominion-KX2_Port1	Not Available
2	Dominion-KX2_Port2	Not Available
3	Dominion-KX2_Port3	Not Available
4	Dominion-KX2_Port4	Not Available
5	JLtestPC	DCIM
6	Dominion-KX2_Port6	Not Available
7	Dominion-KX2_Port7	Not Available
8	Dominion-KX2_Port8	Not Available
9	Local Port	VM
10	Dominion-KX2_Port10	Not Available
11	Dominion-KX2_Port11	Not Available
12	Dominion-KX2_Port12	Not Available
13	Dominion-KX2_Port13	Not Available
14	Dominion-KX2_Port14	Not Available
15	Dominion-KX2_Port15	Not Available
16	PowerStrip	PowerStrip

Copyright © 2007 Raritan Computer Inc.

2. Click the Port Name for the KVM port you want to edit.

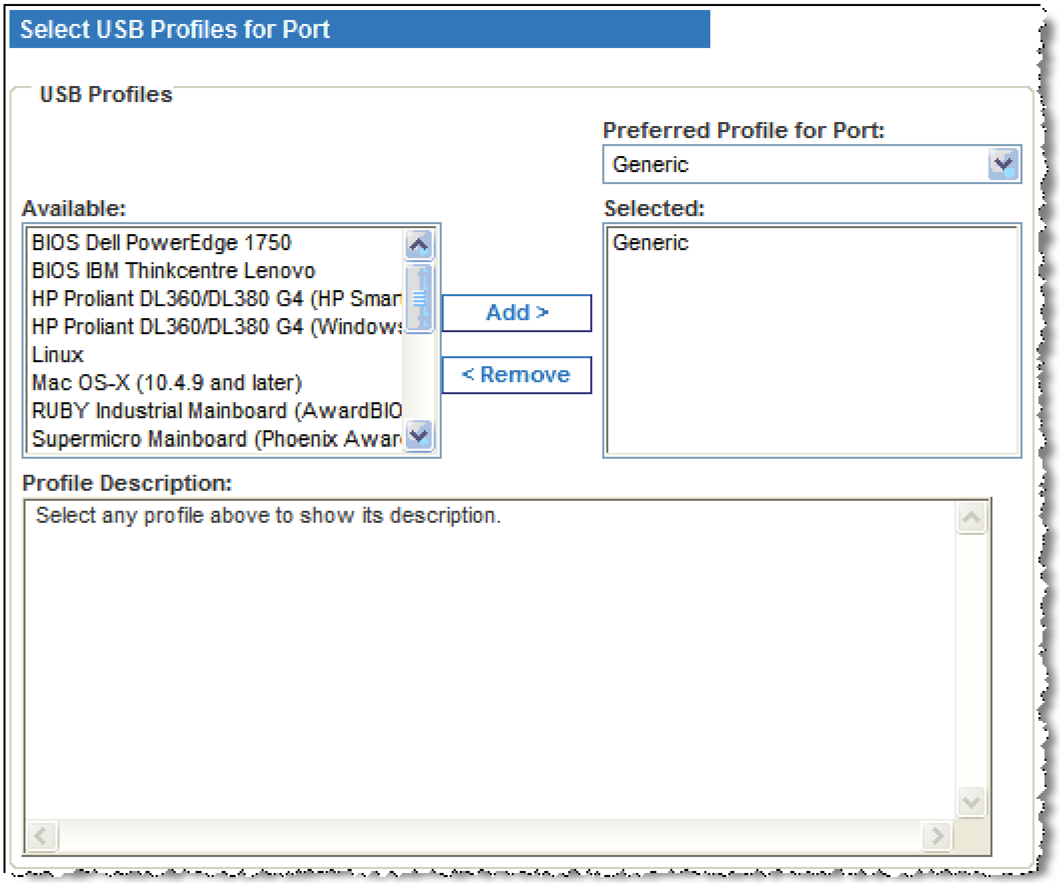
   The Port page opens.

➢ *To select the USB profiles for a KVM port:*

1. In the Select USB Profiles for Port section, select one or more USB profiles from the Available list.

   - Shift-Click and drag to select several continuous profiles.

- Ctrl-Click to select several discontinuous profiles.



Select USB Profiles for Port

USB Profiles

Preferred Profile for Port: Generic

Available:

BIOS Dell PowerEdge 1750
BIOS IBM Thinkcentre Lenovo
HP Proliant DL360/DL380 G4 (HP Smar
HP Proliant DL360/DL380 G4 (Window
Linux
Mac OS-X (10.4.9 and later)
RUBY Industrial Mainboard (AwardBIO
Supermicro Mainboard (Phoenix Awar

Selected:

Generic

Profile Description:

Select any profile above to show its description.

2. Click Add.

   The selected profiles appear in the Selected list. These are the profiles that can be use for the KVM target server connected to the port.

➢ *To specify a preferred USB profile:*

1. After selecting the available profiles for a port, choose one from the Preferred Profile for Port menu. The default is Generic.

   The selected profile will be used when connecting to the KVM target server. You can change to any other USB profile as necessary.

➢ *To remove selected USB profiles:*

1. In the Select USB Profiles for Port section, select one or more profiles from the Selected list.

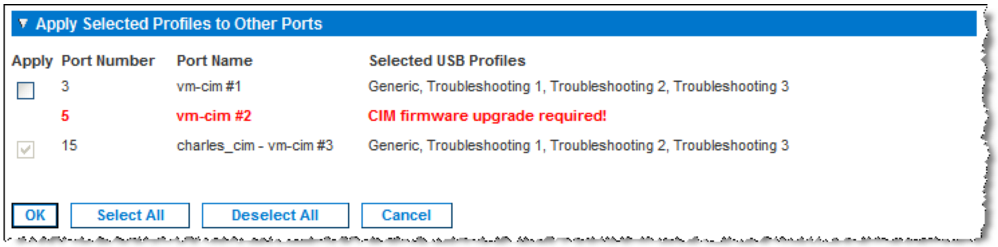
   - Shift-Click and drag to select several continuous profiles.
   - Ctrl-Click to select several discontinuous profiles.

2. Click Remove.

   The selected profiles appear in the Available list. These profiles are no longer available for a KVM target server connected to this port.

➢ *To apply a profile selection to multiple ports:*

1. In the Apply Selected Profiles to Other Ports section, select the Apply checkbox for each KVM port you want to apply the current set of selected USB profiles to.



▼ Apply Selected Profiles to Other Ports

Apply	Port Number	Port Name	Selected USB Profiles
☐	3	vm-cim #1	Generic, Troubleshooting 1, Troubleshooting 2, Troubleshooting 3
	5	vm-cim #2	CIM firmware upgrade required!
☑	15	charles_cim - vm-cim #3	Generic, Troubleshooting 1, Troubleshooting 2, Troubleshooting 3

- To select all KVM ports, click Select All.
- To deselect all KVM ports, click Deselect All.

Chapter 8 Security Settings

In This Chapter

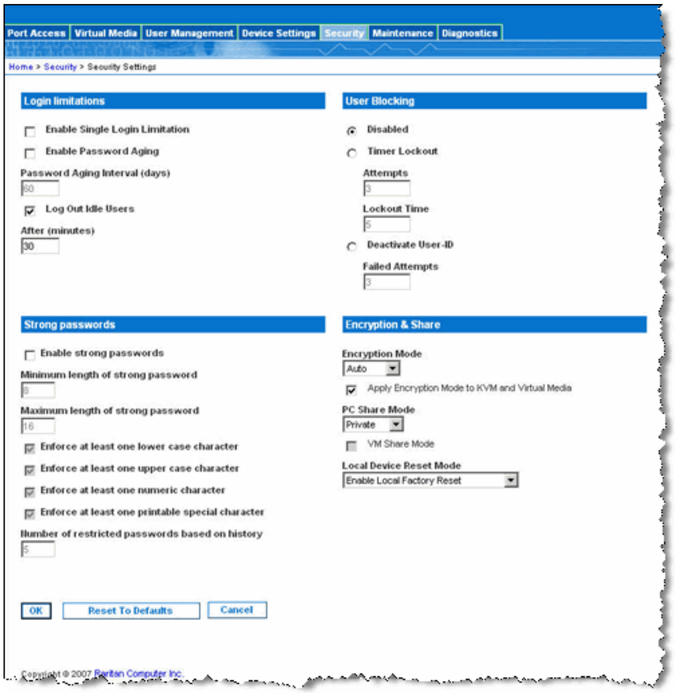
Security Settings

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

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

➢ *To configure the security settings:*

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



Login limitations

☐ Enable Single Login Limitation

☐ Enable Password Aging

Password Aging Interval (days): 60

☑ Log Out Idle Users

After (minutes): 30

User Blocking

● Disabled

○ Timer Lockout

Attempts: 3

Lockout Time: 5

○ Deactivate User-ID

Failed Attempts: 3

Strong passwords

☐ Enable strong passwords

Minimum length of strong password: 8

Maximum length of strong password: 16

☑ Enforce at least one lower case character

☑ Enforce at least one upper case character

☑ Enforce at least one numeric character

☑ Enforce at least one printable special character

Number of restricted passwords based on history: 5

Encryption & Share

Encryption Mode: Auto

☑ Apply Encryption Mode to KVM and Virtual Media

PC Share Mode: Private

☐ VM Share Mode

Local Device Reset Mode: Enable Local Factory Reset

Copyright © 2007 Raritan Computer Inc.

2. Update the ***Logon Limitations*** (on page 249) settings as appropriate.
3. Update the ***Strong Passwords*** (on page 250) settings as appropriate.
4. Update the ***User Blocking*** (on page 251) settings as appropriate.
5. Update the Encryption & Share settings as appropriate.
6. Click OK.

➢ ***To reset back to defaults:***

- Click Reset to Defaults.

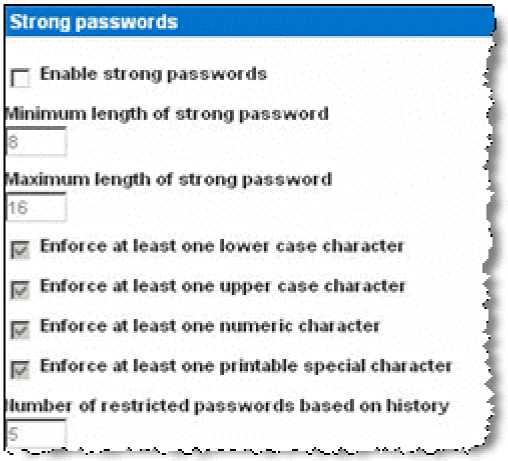
Logon Limitations

Using logon limitations you can specify restrictions for single logon, password aging, and the logging off of idle users.

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

Strong Passwords

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



Strong passwords

□ Enable strong passwords

Minimum length of strong password: 8

Maximum length of strong password: 16

☑ Enforce at least one lower case character

☑ Enforce at least one upper case character

☑ Enforce at least one numeric character

☑ Enforce at least one printable special character

Number of restricted passwords based on history: 5

Strong passwords require user-created passwords to have a minimum of 8 characters with at least one alphabetical character and one nonalphabetical character (punctuation character or number). In addition, the first four characters of the password and the user name cannot match.

When selected, strong password rules are enforced. Users with passwords not meeting strong password criteria will automatically be required to change their password on their next login. When deselected, only the standard format validation is enforced. When selected, the following fields are enabled and required:

Field	Description
Minimum length of strong password	Passwords must be at least 8 characters long. The default is 8, but it can be up to 63.
Maximum length of strong password	The default is 16, but can be up to 64 characters long.
Enforce at least one lower case character	When checked, at least one lower case character is required in the password.
Enforce at least one upper case character	When checked, at least one upper case character is required in the password.

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

User Blocking

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

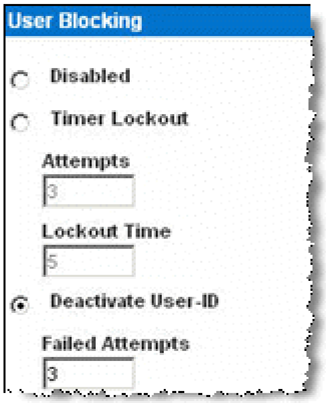
The three options are mutually exclusive:

Option	Description
Disabled	The default option; users are not blocked regardless of the number of times they fail authentication.

User Blocking

Option	Description
Timer Lockout	Users are denied access to the system for the specified amount of time after exceeding the specified number of unsuccessful login attempts. When selected, the following fields are enabled: Attempts - The number of unsuccessful login attempts after which the user will be locked out. The valid range is 1 - 10; the default is 3 attempts. Lockout Time - The amount of time for which the user will be locked out. The valid range is 1 - 1440 minutes; the default is 5 minutes.
Deactivate User-ID	When selected, this option specifies that the user will be locked out of the system after the number of failed login attempts specified in the Failed Attempts field: Failed Attempts - The number of unsuccessful login attempts after which the user's User-ID will be deactivated. This field is enabled when the Deactivate User-ID option is selected. The valid range is 1 - 10.

When a user-ID is deactivated after the specified number of failed attempts, the administrator must change the user password and activate the user account by selecting the Active checkbox on the User page.



User Blocking

○ Disabled

○ Timer Lockout

Attempts: 3

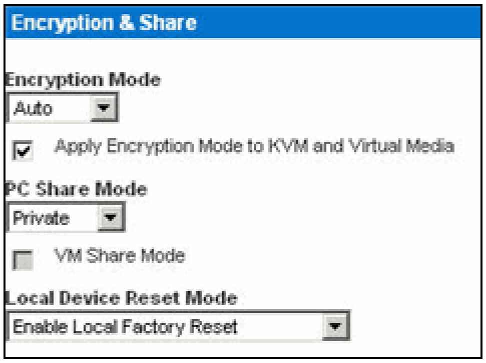
Lockout Time: 5

● Deactivate User-ID

Failed Attempts: 3

Encryption & Share

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



Encryption & Share

Encryption Mode

Auto

☑ Apply Encryption Mode to KVM and Virtual Media

PC Share Mode

Private

□ VM Share Mode

Local Device Reset Mode

Enable Local Factory Reset

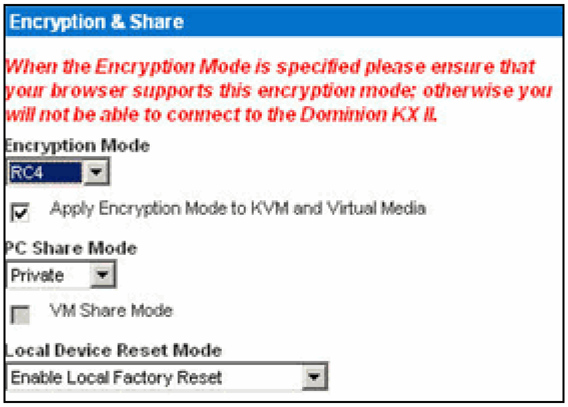
Choose one of the options from the drop-down list. When an encryption mode is selected, a warning is displayed that if your browser does not support the selected mode, you will not be able to connected to the Dominion KX II.

Encryption mode	Description
Auto	This is the recommended option; the Dominion KX II autonegotiates to the highest level of encryption possible.
RC4	Secures user names, passwords and KVM data, including video transmissions using the RSA RC4 encryption method. This is a 128-bit Secure Sockets Layer (SSL) protocol that provides a private communications channel between the Dominion KX II unit and the Remote PC during initial connection authentication.
AES-128	The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data; 128 is the key length. When AES-128 is specified, be certain that your browser supports it, otherwise you will not be able to connect. Refer to *Checking Your Browser for AES Encryption* (on page 255) for more information.

Note: If you are running Windows XP with Service Pack 7, Internet Explorer 7 cannot connect remotely to the Dominion KX II using AES-128 encryption.

- Apply Encryption Mode to KVM and Virtual Media. When selected, this option applies the selected encryption mode to both KVM and virtual media. After authentication, KVM and virtual media data is also transferred with 128-bit encryption.
- PC Share Mode. Determines global concurrent remote KVM access, enabling up to eight remote users to simultaneously log on to one Dominion KX II and concurrently view and control the same target server through the device. Click the drop-down list to select one of the following options:
  - Private: No PC share; this is the default mode. Each target server can be accessed exclusively by only one user at a time.
  - PC-Share: KVM target servers can be accessed by up to eight users (administrator or non-administrator) at one time. Each remote user has equal keyboard and mouse control, however, note that uneven control will occur if one user does not stop typing or moving the mouse.
- VM Share Mode. This option is enabled only when PC-Share mode is enabled. When selected, this option permits the sharing of virtual media among multiple users, that is, several users can access the same virtual media session. The default is disabled.
- Local Device Reset Mode. This option specifies which actions are taken when the hardware Reset button (at the back of the unit) is depressed. For more information, refer to ***Resetting the Dominion KX II Using the Reset Button*** (on page 287). Choose one of the following options:

PC Share mode	Description
Enable Local Factory Reset (default)	Returns the Dominion KX II unit to the factory defaults.
Enable Local Admin Password Reset	Resets the local administrator password only. The password is reset to raritan.
Disable All Local Resets	No reset action is taken.



Encryption & Share

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

Encryption Mode
RC4

☑ Apply Encryption Mode to KVM and Virtual Media

PC Share Mode
Private

☐ VM Share Mode

Local Device Reset Mode
Enable Local Factory Reset

Checking Your Browser for AES Encryption

If you do not know if your browser uses AES, check with the browser manufacturer or navigate to the https://www.fortify.net/sslcheck.html website using the browser with the encryption method you want to check. This website detects your browser's encryption method and displays a report.

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

AES 256 Prerequisites and Supported Configurations

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

- Firefox 2.0.0.x
- Mozilla 1.7.13
- Internet Explorer 7

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

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

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

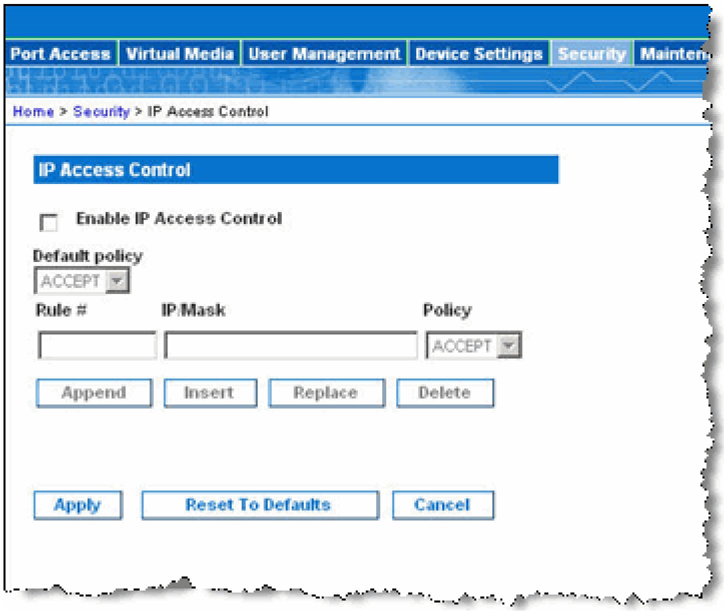
IP Access Control

Using IP access control, you can control access to your Dominion KX II. By setting a global Access Control List (ACL) you are by ensuring that your device does not respond to packets being sent from disallowed IP addresses. The IP access control is global, affecting the Dominion KX II as a whole, but you can also control access to your device at the group level. Refer to ***Group-based IP ACL (Access Control List)*** (on page 201) for more information about group-level control.

Important: IP address 127.0.0.1 is used by the Dominion KX II local port. When creating an IP Access Control list, if 127.0.0.1 is within the range of IP addresses that are blocked, you will not have access to the Dominion KX II local port.

➢ *To use IP Access Control:*

1. Open the IP Access Control page using one of these methods by selecting Security > IP Access Control or clicking the Set System ACL button from the ***Network Settings*** (on page 219) page. The IP Access Control page opens.



□ Enable IP Access Control

Default policy: ACCEPT

Rule #	IP/Mask	Policy
		ACCEPT

2. Select the Enable IP Access Control checkbox to enable IP access control and the remaining fields on the page.

3. Choose the Default Policy. This is the action taken for IP addresses that are not within the ranges you specify.

- Accept. IP addresses are allowed access to the Dominion KX II device.
- Drop. IP addresses are denied access to the Dominion KX II device.

➢ *To add (append) rules:*

1. Type the IP address and subnet mask in the IP/Mask field.

   Note: The IP address should be entered using CIDR (Classless Inter-Domain Routing notation, in which the first 24 bits are used as a network address).

2. Choose the Policy from the drop-down list.
3. Click Append. The rule is added to the bottom of the rules list.

➢ *To insert a rule:*

1. Type a rule #. A rule # is required when using the Insert command.
2. Type the IP address and subnet mask in the IP/Mask field.
3. Choose the Policy from the drop-down list.
4. Click Insert. If the Rule # you just typed equals an existing rule #, the new rule is placed ahead of the exiting rule and all rules are moved down in the list.

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

➢ *To replace a rule:*

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

➢ *To delete a rule:*

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

Chapter 9 Maintenance

In This Chapter

Audit Log

A log is created of Dominion KX II system events.

➢ *To view the audit log for your Dominion KX II:*

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

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

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

➢ *To save the audit log:*

Note: Saving the audit log is available only on the Dominion KX II Remote Console, not on the Local Console.

1. Click the Save to File button. A Save File dialog appears.
2. Choose the desired file name and location and click Save. The audit log is saved locally on your client machine with the name and location specified.

➢ *To page through the audit log:*

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

Device Information

The Device Information page provides detailed information about your Dominion KX II device and the CIMs in use. This information is helpful should you need to contact Raritan Technical Support.

➢ ***To view information about your Dominion KX II and CIMs:***

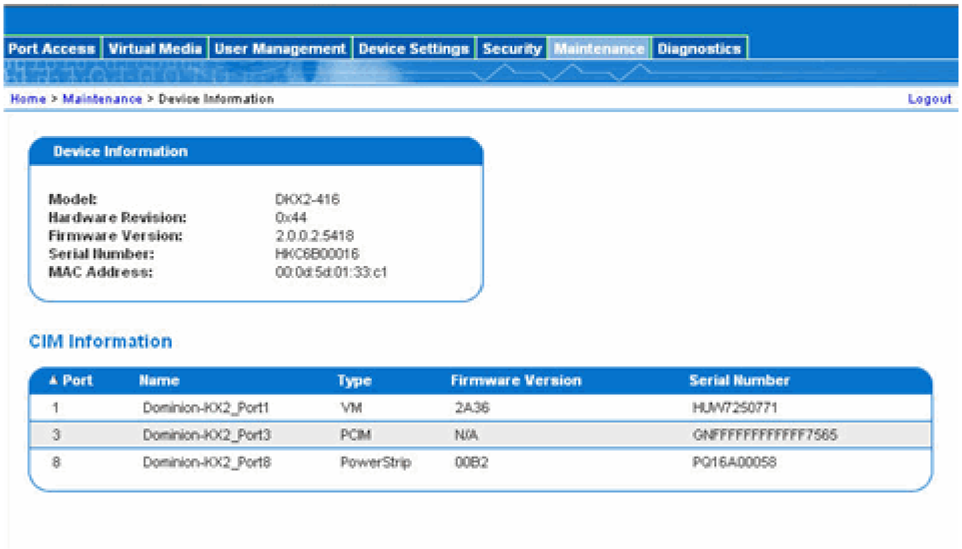
- Choose Maintenance > Device Information. The Device Information page opens.

The following information is provided about the Dominion KX II:

- Model
- Hardware Revision
- Firmware Version
- Serial Number
- MAC Address

The following information is provided about the CIMs in use:

- Port (number)
- Name
- Type of CIM - DCIM, PCIM, Power Strip, or VM
- Firmware Version
- Serial Number



Device Information

Model:	DKX2-416
Hardware Revision:	0x44
Firmware Version:	2.0.0.2.5418
Serial Number:	HKC6B00016
MAC Address:	00:0d:5d:01:33:c1

CIM Information

▲ Port	Name	Type	Firmware Version	Serial Number
1	Dominion-KX2_Port1	VM	2A36	HUW7250771
3	Dominion-KX2_Port3	PCIM	N/A	GNFFFFFFFFFFFF7565
8	Dominion-KX2_Port8	PowerStrip	00B2	PQ16A00058

Figure 1: Device Information

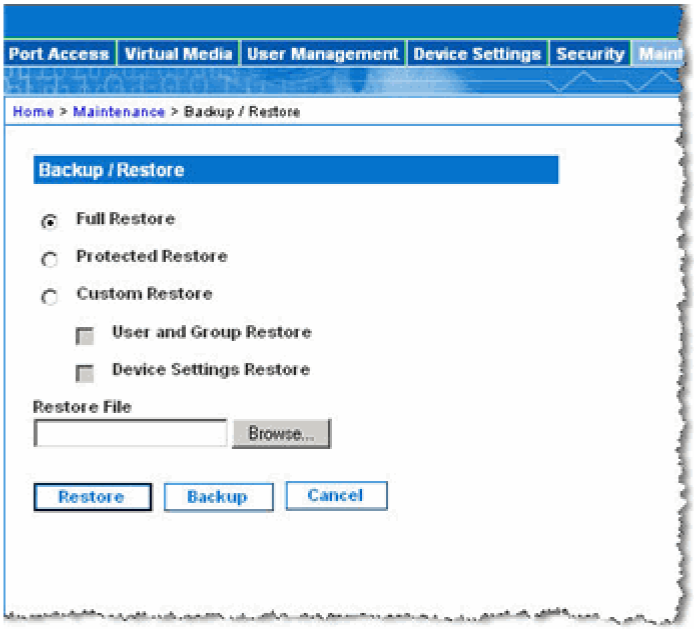
Backup and Restore

From the Backup/Restore page, you can backup and restore the settings and configuration for your Dominion KX II.

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

➢ *To access the Backup/Restore page:*

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



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

➢ *To backup your Dominion KX II:*

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

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

➢ *To restore your Dominion KX II:*

WARNING: Exercise caution when restoring your Dominion KX II to an earlier version. Usernames and password in place at the time of the backup will be restored. If you do not remember the old administrative usernames and passwords, you will be locked out of the Dominion KX II.

In addition, if you used a different IP address at the time of the backup, that IP address will be restored as well. If the configuration uses DHCP, you may want to perform this operation only when you have access to the local port to check the IP address after the update.

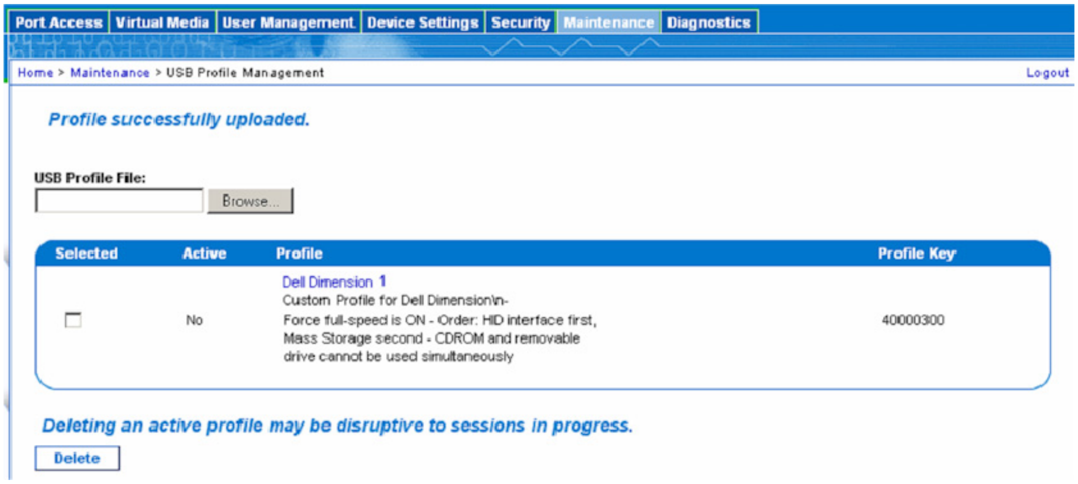
1. Choose the type of restore you want to run:
   - Full Restore - A complete restore of the entire system; generally used for traditional backup and restore purposes.
   - Protected Restore - Everything is restored except device-specific information such as serial number, MAC Address, IP address, name, and so forth. With this option, you can setup one Dominion KX II and copy the configuration to multiple Dominion KX II devices.
   - Custom Restore - With this option, you can select User and Group Restore, Device Settings Restore, or both. Select the appropriate checkboxes:
     - User and Group Restore - This option includes only user and group information. Use this option to quickly set up users on a different Dominion KX II.
     - Device Settings Restore - This option includes only device settings. Use this option to quickly copy the device information.
2. Click the Browse button. A Choose File dialog appears.
3. Navigate to and select the appropriate backup file and click Open. The selected file is listed in the Restore File field.
4. Click Restore. The configuration (based on the type of restore selected) is restored.

USB Profile Management

From the USB Profile Management page, you can upload custom profiles provided by Raritan tech support. These profiles are designed to address the needs of your target server's configuration, in the event that the set of standard profiles does not already address them. Raritan tech support will provide the custom profile and work with you to verify the solution for your target server's specific needs.

➢ *To access the USB Profile Management page:*

- Choose > Maintenance > USB Profile Management. The USB Profile Management page opens.



Profile successfully uploaded.

USB Profile File:

Selected	Active	Profile	Profile Key
□	No	Dell Dimension 1 Custom Profile for Dell Dimension\n- Force full-speed is ON - Order: HID interface first, Mass Storage second - CDROM and removable drive cannot be used simultaneously	40000300

Deleting an active profile may be disruptive to sessions in progress.

➢ *To upload a custom profile to your Dominion KX II:*

1. Click the Browse button. A Choose File dialog appears.
2. Navigate to and select the appropriate custom profile file and click Open. The file selected is listed in the USB Profile File field.
3. Click Upload. The custom profile will be uploaded and displayed in the Profile table.

Note: If an error or warning is displayed during the upload process (for example. overwriting an existing custom profile), you may decided to continue with the upload by clicking on Upload or cancel by clicking on Cancel.

➢ *To delete a custom profile to your Dominion KX II:*

1. Check the box corresponding to the row of the table containing the custom profile to be deleted.

2. Click Delete. The custom profile will be deleted and removed from the Profile table.

As noted, you may delete a custom profile from the system while it is still designated as an active profile. Doing so will terminate any Virtual Media sessions that were in place.

Handling Conflicts in Profile Names

A naming conflict between custom and standard USB profiles may occur when a firmware upgrade is performed. This may occur if a custom profile that has been created and incorporated into the list of standard profiles has the same name as a new USB profile that is downloaded as part of the firmware upgrade.

Should this occur, the preexisting custom profile will be tagged as 'old'. For example, if a custom profile called GenericUSBProfile5 has been created and a profile with the same name is downloaded during a firmware upgrade, the existing file will then be called 'old.GenericUSBProfile5'.

You can delete the existing profile if needed. See ***USB Profile Management*** (on page 262) for more information.

Upgrading CIMs

Use this procedure to upgrade CIMs using the firmware versions stored in the memory of your Dominion KX II unit. In general, all CIMs are upgraded when you upgrade the device firmware using the Firmware Upgrade page.

In order to make use of USB profiles, you must use a D2-CIM VUSB or D2-CIM DVUSB with updated firmware. A VM-CIM that has not had its firmware upgraded will support a broad range of configurations (Windows, Keyboard, Mouse, CD-ROM, and Removable Device) but will not be able to make use of profiles optimized for particular target configurations. Given this, existing VM-CIMs should be upgraded with the latest firmware in order to access USB profiles. Until existing VM-CIMs are upgraded, they will be able to provide functionality equivalent to the 'Generic' profile.

Note: Only D2CIM-VUSB can be upgraded from this page.

➢ ***To upgrade CIMs using the Dominion KX II memory:***

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

   The Port (number), Name, Type, Current CIM Version, and Upgrade CIM Version are displayed for easy identification of the CIMs.

2. Check the Selected checkbox for each CIM you want to upgrade.

   Tip: Use the Select All and Deselect All buttons to quickly select all (or deselect all) of the CIMs.

3. Click the Upgrade button. You are prompted to confirm the upgrade.
4. Click OK to continue the upgrade. Progress bars are displayed during the upgrade. Upgrading takes approximately 2 minutes or less per CIM.

Upgrading Firmware

Use the Firmware Upgrade page to upgrade the firmware for your Dominion KX II unit and all attached CIMs. This page is available in the Dominion KX II Remote Console only.

Important: Do not turn off your Dominion KX II unit or disconnect CIMs while the upgrade is in progress - doing so will likely result in

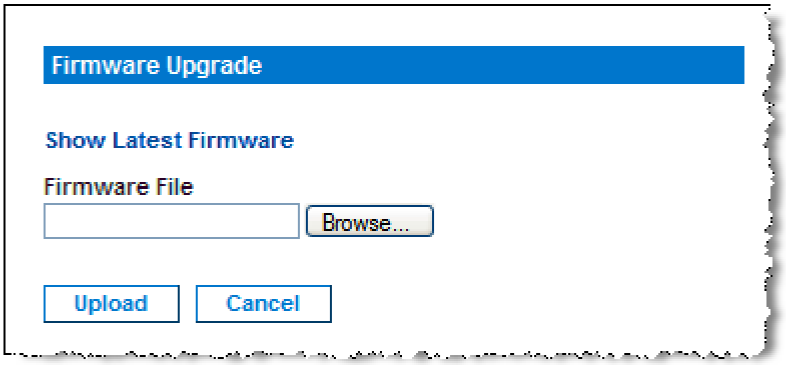
damage to the unit or CIMs.

➢ *To upgrade your Dominion KX II unit:*

1. Locate the appropriate Raritan firmware distribution file (*.RFP) on the Raritan website (www.raritan.com) on the Firmware Upgrades web page.
2. Unzip the file. Please read all instructions included in the firmware ZIP files carefully before upgrading.

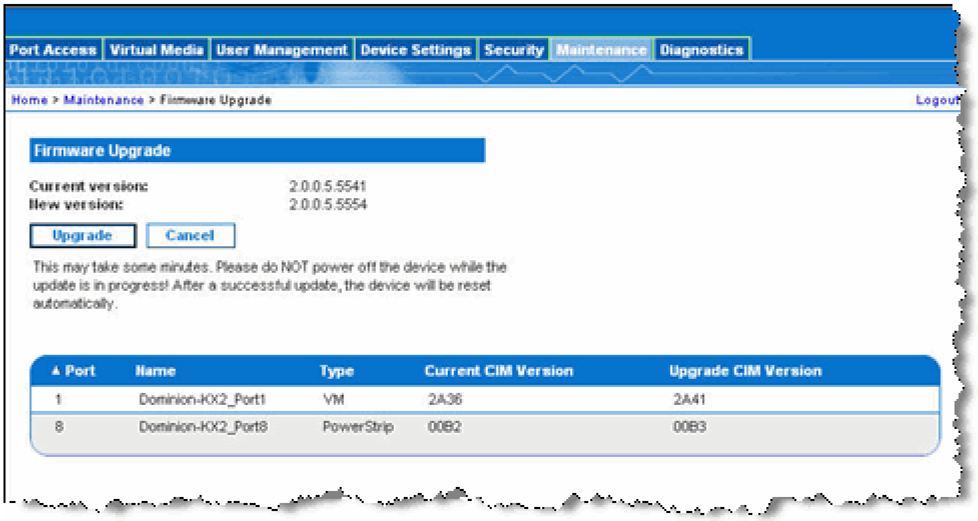
   Note: Copy the firmware update file to a local PC before uploading. Do not load the file from a network drive.

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



4. Click the Browse button to navigate to the directory where you unzipped the upgrade file.
5. Select the Review CIM Version Information? checkbox if you would like information displayed about the versions of the CIMs in use.

6. Click Upload from the Firmware Upgrade page. Information about the upgrade and version numbers is displayed for your confirmation (if you opted to review CIM information, that information is displayed as well):



Firmware Upgrade

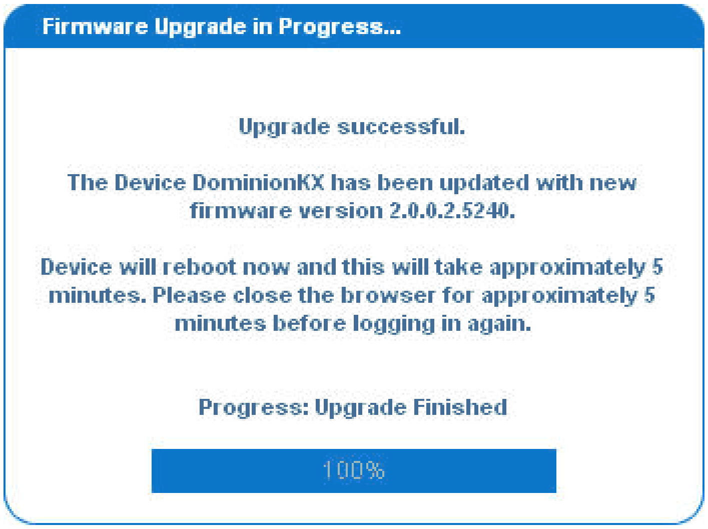
Current version: 2.0.0.5.5541
New version: 2.0.0.5.5554

This may take some minutes. Please do NOT power off the device while the update is in progress! After a successful update, the device will be reset automatically.

▲ Port	Name	Type	Current CIM Version	Upgrade CIM Version
1	Dominion-KX2_Port1	VM	2A36	2A41
8	Dominion-KX2_Port8	PowerStrip	00B2	00B3

Note: At this point, connected users are logged out, and new login attempts are blocked.

7. Click Upgrade. Please wait for the upgrade to complete. Status information and progress bars are displayed during the upgrade. Upon completion of the upgrade, the unit reboots (1 beep sounds to signal that the reboot has completed).



Firmware Upgrade in Progress...

Upgrade successful.

The Device DominionKX has been updated with new firmware version 2.0.0.2.5240.

Device will reboot now and this will take approximately 5 minutes. Please close the browser for approximately 5 minutes before logging in again.

Progress: Upgrade Finished

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

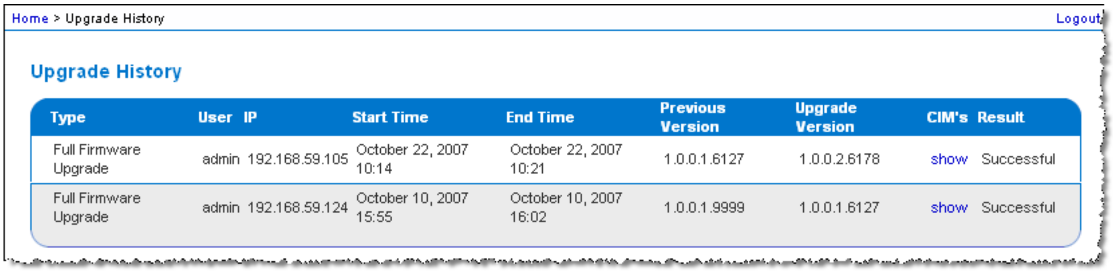
For information about upgrading the device firmware using the Multi-Platform Client, refer to ***Upgrading Device Firmware*** (on page 163).

Upgrade History

The Dominion KX II provides information about upgrades performed on the Dominion KX II and attached CIMS.

➢ ***To view the upgrade history:***

- Choose Maintenance > Upgrade History. The Upgrade History page opens.



Upgrade History

Type	User	IP	Start Time	End Time	Previous Version	Upgrade Version	CIM's	Result
Full Firmware Upgrade	admin	192.168.59.105	October 22, 2007 10:14	October 22, 2007 10:21	1.0.0.1.6127	1.0.0.2.6178	show	Successful
Full Firmware Upgrade	admin	192.168.59.124	October 10, 2007 15:55	October 10, 2007 16:02	1.0.0.1.9999	1.0.0.1.6127	show	Successful

Information is provided about the Dominion KX II upgrade(s) that have been run, the final status of the upgrade, the start and end times, and the previous and current firmware versions. Information is also provided about the CIMS, which can be obtained by clicking the show link for an upgrade. The CIM information provided is:

- Port - The port where the CIM is connected.
- Type - The type of CIM.
- Result - The result of the upgrade (success or fail).
- Current Version - The CIM firmware version.

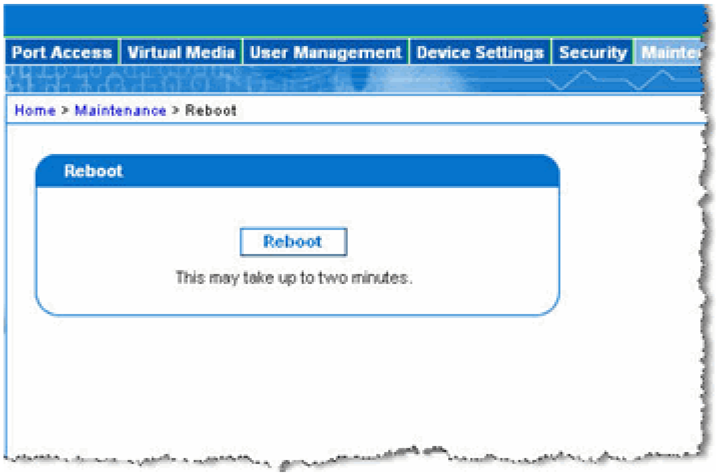
Rebooting

The Reboot page provides a safe and controlled way to reboot your Dominion KX II. This is the recommended method for rebooting.

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

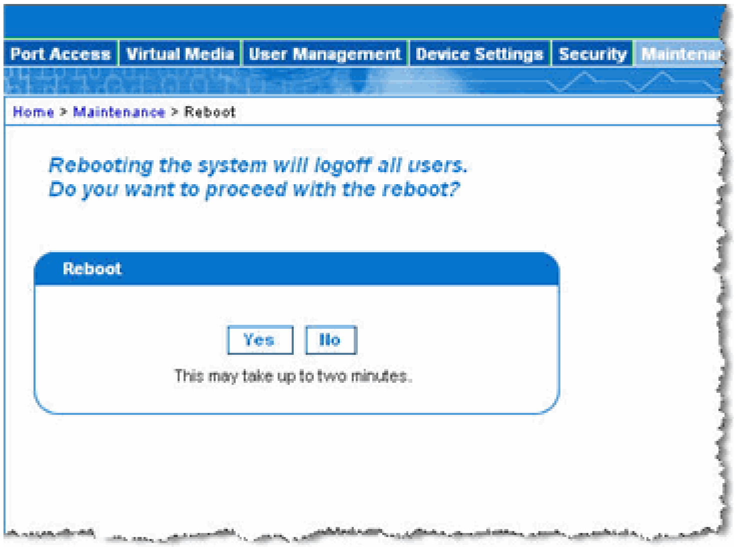
➢ *To reboot your Dominion KX II:*

1. Choose Maintenance > Reboot. The Reboot page opens.



This may take up to two minutes.

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



Rebooting the system will logoff all users.
Do you want to proceed with the reboot?

This may take up to two minutes.

3. Click Yes to proceed with the reboot.

Chapter 10 Diagnostics

The Diagnostics pages are used for troubleshooting and are intended primarily for the administrator of the Dominion KX II device. All of the Diagnostics pages (except Device Diagnostics) run standard networking commands; the information displayed is the output of those commands. The Diagnostics menu options help you debug and configure the network settings.

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

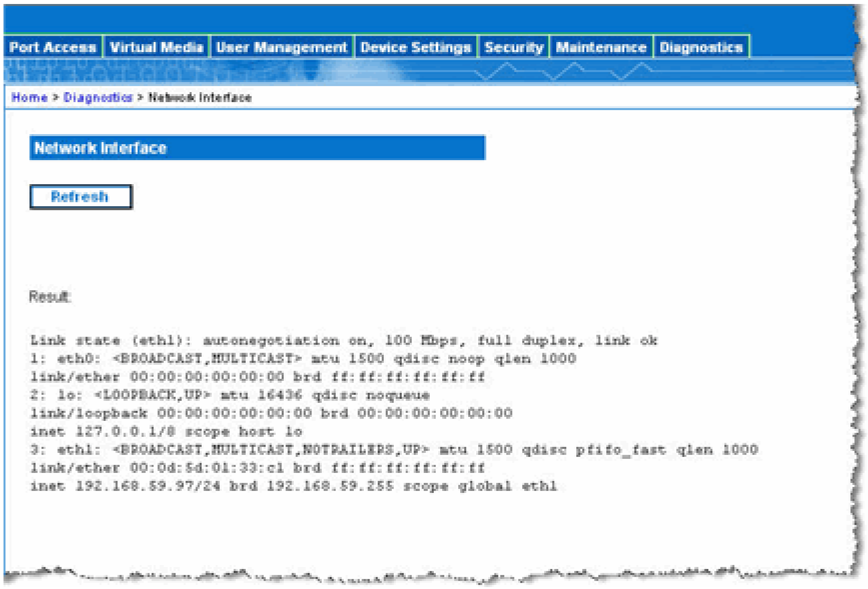
In This Chapter

Network Interface Page

The Dominion KX II provides information about the status of your network interface.

➢ ***To view information about your network interface:***

- Choose Diagnostics > Network Interface. The Network Interface page opens.



Result:

```
Link state (eth1): autonegotiation on, 100 Mbps, full duplex, link ok
1: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
2: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
3: eth1: <BROADCAST,MULTICAST,NOTRAILERS,UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0d:5d:01:33:c1 brd ff:ff:ff:ff:ff:ff
inet 192.168.59.97/24 brd 192.168.59.255 scope global eth1
```

The following information is displayed:

- Whether the Ethernet interface is up or down.
- Whether the gateway is pingable or not.
- The LAN port that is currently active.

➢ ***To refresh this information:***

- Click the Refresh button.

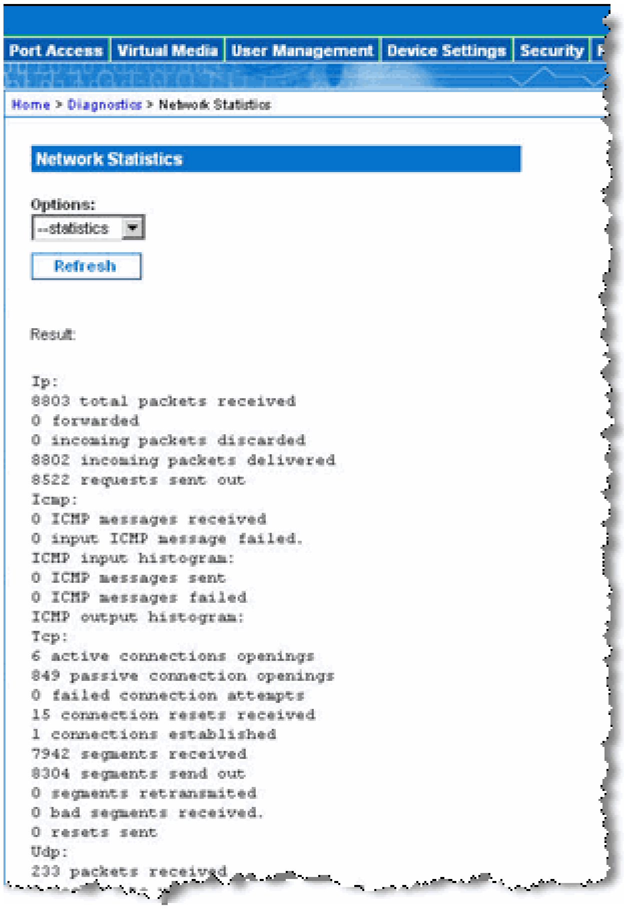
Network Statistics Page

The Dominion KX II provides statistics about your network interface.

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

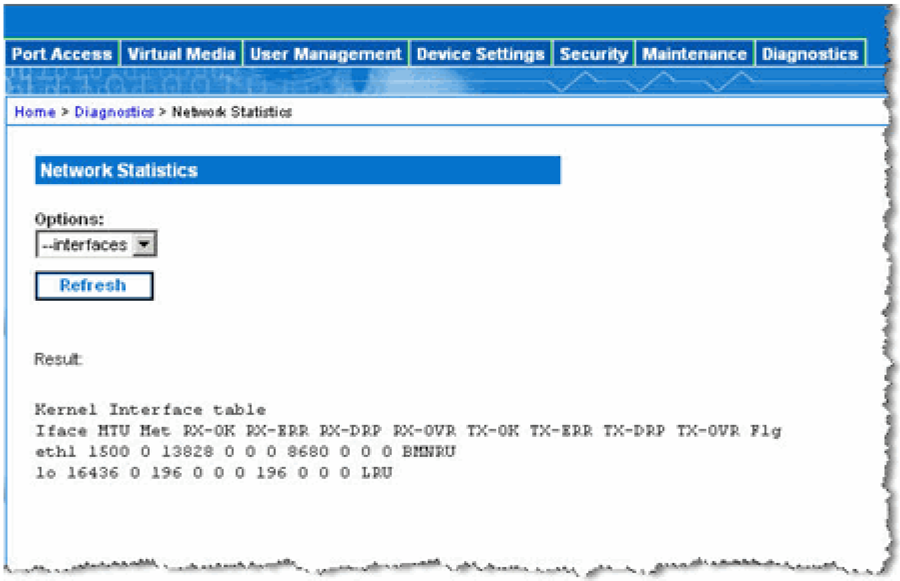
1. Choose Diagnostics > Network Statistics. The Network Statistics page opens.
2. Choose the appropriate option from the Options drop-down list:

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



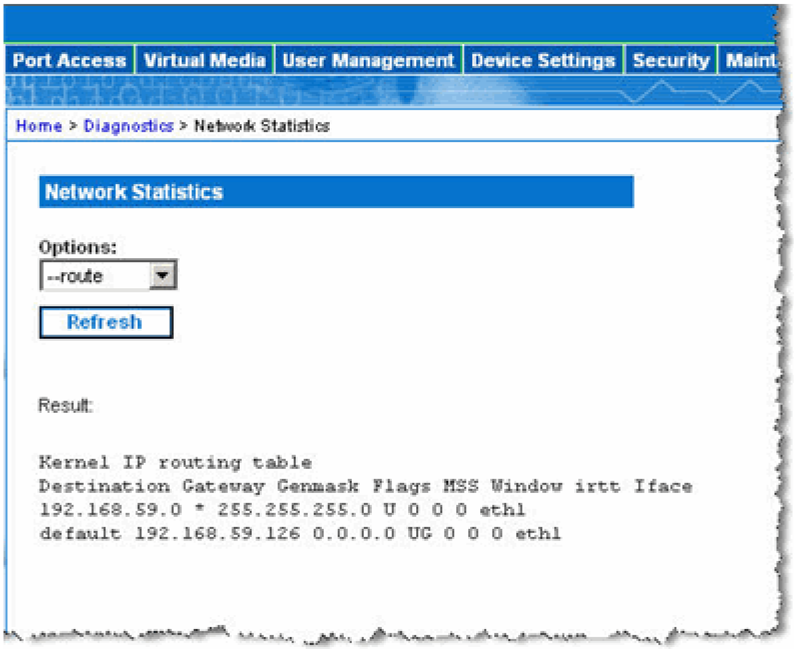
```
Ip:
8803 total packets received
0 forwarded
0 incoming packets discarded
8802 incoming packets delivered
8522 requests sent out
Icmp:
0 ICMP messages received
0 input ICMP message failed.
ICMP input histogram:
0 ICMP messages sent
0 ICMP messages failed
ICMP output histogram:
Tcp:
6 active connections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

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



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

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



```
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
192.168.59.0 * 255.255.255.0 U 0 0 0 eth1
default 192.168.59.126 0.0.0.0 UG 0 0 0 eth1
```

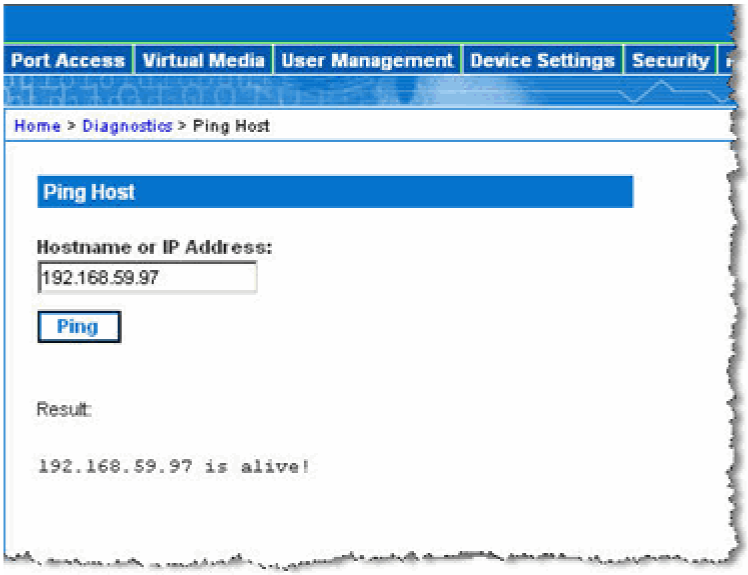
3. Click the Refresh button. The relevant information is displayed in the Result field.

Ping Host Page

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

➤ ***To ping the host:***

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



Hostname or IP Address: 192.168.59.97

Result:

```
192.168.59.97 is alive!
```

2. Type either the hostname or IP address into the Hostname or IP Address field.

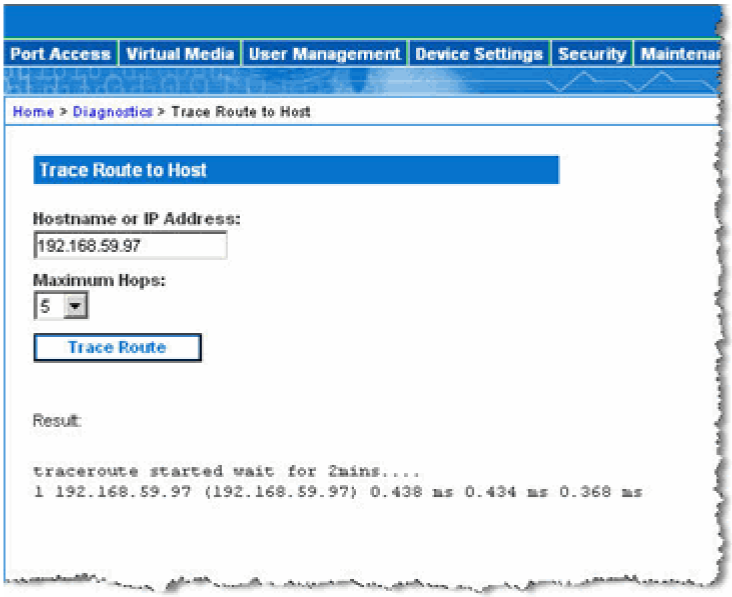
3. Click Ping. The results of the ping are displayed in the Result field.

Trace Route to Host Page

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

➢ *To trace the route to the host:*

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



Hostname or IP Address: 192.168.59.97

Maximum Hops: 5

Result:

```
traceroute started wait for 2mins....
1 192.168.59.97 (192.168.59.97) 0.438 ms 0.434 ms 0.368 ms
```

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

Device Diagnostics

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

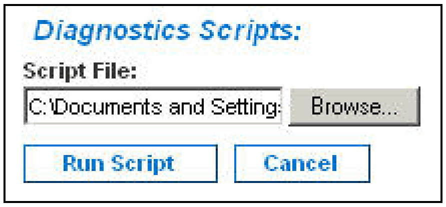
Device diagnostics downloads the diagnostics information from the Dominion KX II to the client machine. Two operations can be performed on this page:

- Execute a special diagnostics script to provided by Raritan Technical Support during a critical error debugging session. The script is uploaded to the unit and executed. Once this script has been executed, you can download the diagnostics messages through the Save to File button.
- Download the device diagnostic log for a snapshot of diagnostics messages from the Dominion KX II unit to the client. This encrypted file is then sent to Raritan Technical Support. Only Raritan can interpret this file.

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

➢ *To run the Dominion KX II System diagnostics:*

1. Choose Diagnostics > Dominion KX II Diagnostics. The Dominion KX II Diagnostics page opens.
2. To execute a diagnostics script file emailed to you from Raritan Technical Support:
   a. Retrieve the diagnostics file supplied by Raritan and unzip as necessary.
   b. Use the Browse button. A Choose File dialog box opens.
   c. Navigate to and select the diagnostic file.
   d. Click Open. The file is displayed in the Script File field.

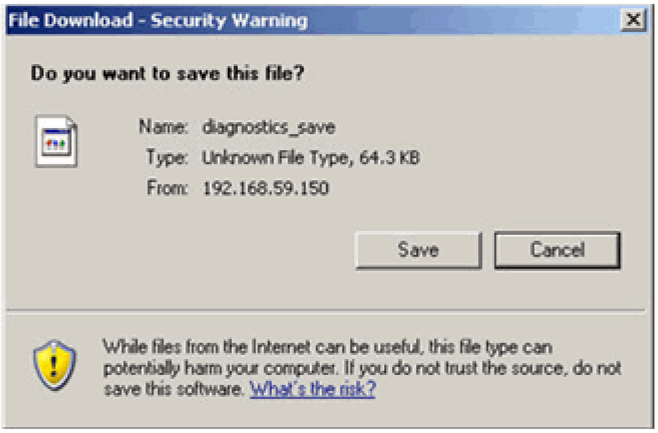


Diagnostics Scripts:

Script File: C:\Documents and Setting

   e. Click Run Script. Send this file to Raritan Technical Support.
3. To create a diagnostics file to send to Raritan Technical Support:

a. Click the Save to File button. The File Download dialog opens.


File Download - Security Warning

Do you want to save this file?

Name: diagnostics_save

Type: Unknown File Type, 64.3 KB

From: 192.168.59.150

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not save this software. What's the risk?

b. Click Save. The Save As dialog box opens.

c. Navigate to the desired directory and click Save.

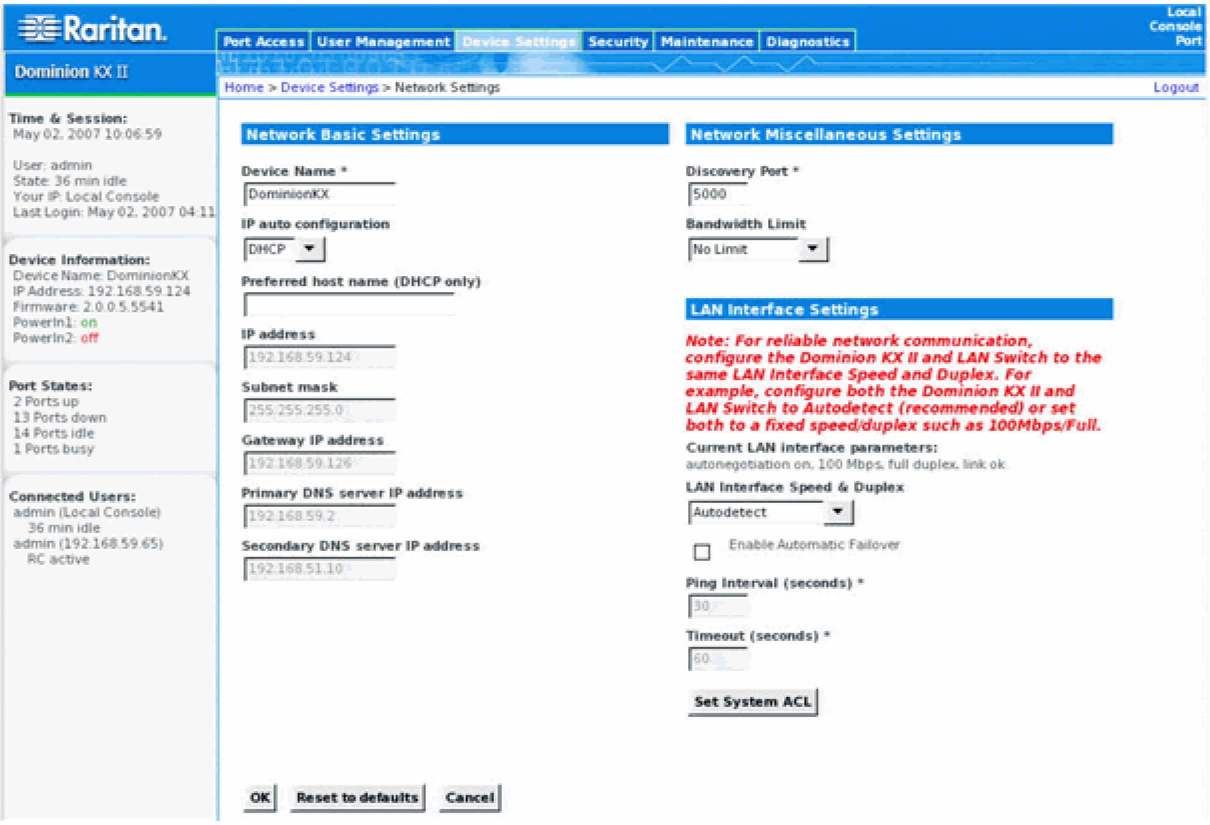
d. Email this file as directed by Raritan Technical Support.

Chapter 11 Dominion KX II Local Console

In This Chapter

Overview

The Dominion KX II provides at-the-rack access and administration via its local port, which features a browser-based graphical user interface for quick, convenient switching between servers. The Dominion KX II Local Console provides a direct analog connection to your connected servers, which provides the same performance is as if you were directly connected to the server's keyboard, mouse, and video ports. The Dominion KX II Local Console provides the same administrative functionality as the Dominion KX II Remote Console.



Time & Session:
May 02, 2007 10:06:59

User: admin
State: 36 min idle
Your IP: Local Console
Last Login: May 02, 2007 04:11

Device Information:
Device Name: DominionKX
IP Address: 192.168.59.124
Firmware: 2.0.0.5.5541
PowerIn1: on
PowerIn2: off

Port States:
2 Ports up
13 Ports down
14 Ports idle
1 Ports busy

Connected Users:
admin (Local Console)
36 min idle
admin (192.168.59.65)
RC active

Network Basic Settings

Device Name *
DominionKX

IP auto configuration
DHCP

Preferred host name (DHCP only)

IP address
192.168.59.124

Subnet mask
255.255.255.0

Gateway IP address
192.168.59.126

Primary DNS server IP address
192.168.59.2

Secondary DNS server IP address
192.168.51.10

Network Miscellaneous Settings

Discovery Port *
5000

Bandwidth Limit
No Limit

LAN Interface Settings

Note: For reliable network communication, configure the Dominion KX II and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX II and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.

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

LAN Interface Speed & Duplex
Autodetect

□ Enable Automatic Failover

Ping Interval (seconds) *
30

Timeout (seconds) *
60

Starting the Dominion KX II Local Console

Simultaneous Users

The Dominion KX II Local Console provides an independent access path to the connected KVM target servers. Using the Local Console does not prevent other users from simultaneously connecting over the network. And even when remote users are connected to the Dominion KX II, you can still simultaneously access your servers from the rack via the Local Console.

Security and Authentication

In order to use the Dominion KX II Local Console, you must first authenticate with a valid user name and password. Dominion KX II provides a fully-integrated authentication and security scheme, whether your access is via the network or the local port. In either case, Dominion KX II allows access only to those servers to which a user has access permissions. Refer to ***User Management*** (on page 196) for additional information on specifying server access and security settings.

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

Note: You can also specify no authentication for Local Console access; this option is recommended only for secure environments.

➢ ***To use the Dominion KX II Local Console:***

1. You need a keyboard, mouse, and video display connected to the local ports at the back of the Dominion KX II.
2. Start the Dominion KX II. The Dominion KX II Local Console interface displays.

Dominion KX II Local Console Interface

The Dominion KX II Local Console interface is almost identical to the Dominion KX II Remote Console interface. Where there are differences, they are noted in the user guide.

Available Resolutions

The Dominion KX II Local Console provides the following resolutions to support various monitors:

- 800x600
- 1024x768
- 1280x1024

Each of these resolutions supports a refresh rate of 60Hz and 75Hz.

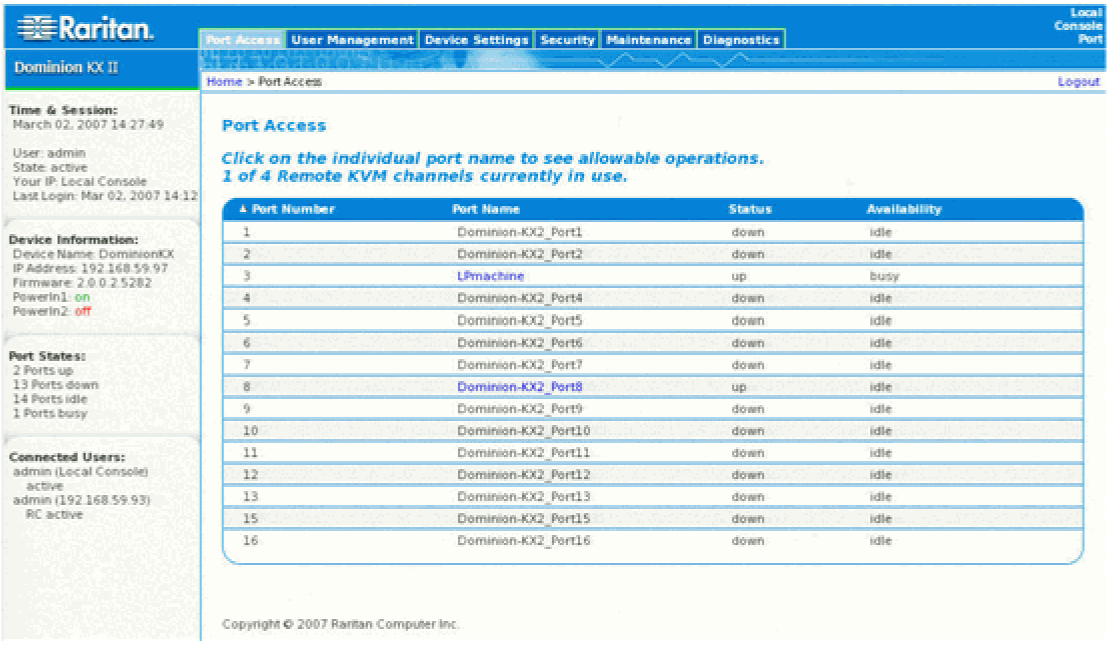
Dominion KX II Local Console Support Languages

The Dominion KX II Local Console supports the following language keyboards: US English, UK English, German, French, Norwegian, Swedish, Danish, Belgium, Japanese, Korean, Simplified Chinese, and Traditional Chinese.

Note: Keyboard use for Chinese, Japanese, and Korean is for display only; local language input is not supported at this time for Dominion KX II Local Console functions.

Server Display

After you login to the Dominion KX II Local Console, the Port Access page opens. This page lists all of the Dominion KX II ports, the connected KVM target servers, and their status and availability.



Time & Session:
March 02, 2007 14:27:49

User: admin
State: active
Your IP: Local Console
Last Login: Mar 02, 2007 14:12

Device Information:
Device Name: DominionKX
IP Address: 192.168.59.97
Firmware: 2.0.0.2.5282
PowerIn1: on
PowerIn2: off

Port States:
2 Ports up
13 Ports down
14 Ports idle
1 Ports busy

Connected Users:
admin (Local Console)
active
admin (192.168.59.93)
RC active

Port Access

Click on the individual port name to see allowable operations.
1 of 4 Remote KVM channels currently in use.

▲ Port Number	Port Name	Status	Availability
1	Dominion-KX2_Port1	down	idle
2	Dominion-KX2_Port2	down	idle
3	LPmachine	up	busy
4	Dominion-KX2_Port4	down	idle
5	Dominion-KX2_Port5	down	idle
6	Dominion-KX2_Port6	down	idle
7	Dominion-KX2_Port7	down	idle
8	Dominion-KX2_Port8	up	idle
9	Dominion-KX2_Port9	down	idle
10	Dominion-KX2_Port10	down	idle
11	Dominion-KX2_Port11	down	idle
12	Dominion-KX2_Port12	down	idle
13	Dominion-KX2_Port13	down	idle
15	Dominion-KX2_Port15	down	idle
16	Dominion-KX2_Port16	down	idle

Copyright © 2007 Raritan Computer Inc.

The KVM target servers are initially sorted by port number but you can change the display to sort on any of the columns.

- Port Number - Numbered from 1 to the total number of ports available for the Dominion KX II unit. Note that ports connected to power strips will not be among those listed, resulting in gaps in the Port Number sequence.
- Port Name - The name of the Dominion KX II port. Initially, this set to Dominion KX II-Port#, but you can change the name to something more descriptive. When you click on the Port Name link, an Action Menu is opened. Refer to the ***Port Action Menu*** (on page 42) for more information about the menu options available.

Note: Do not use apostrophes for the Port (CIM) Name.

- Status - The Status is either up or down.
- Availability - Valid Values per include Idle, Connected, Busy, or Unavailable.

➢ ***To change the sort order:***

- Click the column heading you want to sort on. The list of KVM target servers is sorted by that column.

Hotkeys

Because the Dominion KX II Local Console interface is completely replaced by the interface for the target server you are accessing, a hot key is utilized so you can switch between these interfaces.

The Local Port hot key allows you to rapidly access the Dominion KX II Local Console user interface when a target server is currently being viewed. The default is to press the Scroll Lock key twice in rapid succession, but you can designate another key combination (available in the Local Port Settings page) as the hot key. Refer to ***Dominion KX II Local Console Local Port Settings*** (on page 283) for more information.

Accessing a Target Server

➢ ***To access a target server:***

1. Click the Port Name of the target you want to access. The Port Action Menu is displayed.
2. Choose Connect from the ***Port Action Menu*** (on page 42). The video display switches to the target server interface.

Returning to the Dominion KX II Local Console Interface

Important: The Dominion KX II Local Console default hot key is to press the Scroll Lock key twice rapidly. This key combination can be changed in the Local Port Settings page. See *Dominion KX II Local Console Local Port Settings* **(on page 283).**

➢ ***To return to the Dominion KX II Local Console from the target server:***

- Press the hot key twice rapidly (the default hot key is Scroll Lock) . The video display switches from the target server interface to the Dominion KX II Local Console interface.

Local Port Administration

The Dominion KX II can be managed by either the Dominion KX II Local Console or the Dominion KX II Remote Console. Note that the Dominion KX II Local Console also provides access to these administrative functions:

- Local Port Settings
- Factory Reset

Note: Only users with administrative privileges can access these functions.

Dominion KX II Local Console Local Port Settings

From the Local Port Settings page, you can customize many settings for the Dominion KX II Local Console including keyboard, local port hot key, video switching delay, power save mode, local user interface resolution settings, and local user authentication.

Note: This feature is available only on the Dominion KX II Local Console.

➢ ***To configure the local port settings:***

1. Choose Device Settings > Local Port Settings. The Local Port Settings page opens.
2. Choose the appropriate keyboard type from among the options in the drop-down list:
   - US
   - US/International
   - UK
   - French
   - German
   - JIS (Japanese Industry Standard)
   - Simplified Chinese
   - Traditional Chinese
   - Dubeolsik Hangul (Korean)
   - German
   - Norwegian

- Swedish
- Danish
- Belgian

3. Choose the local port hotkey. The local port hotkey is used to return to the Dominion KX II Local Console interface when a target server interface is being viewed. The default is to Double Click Scroll Lock, but you can select any key combination from the drop-down list:

Hot key:	Take this action:
Double Click Scroll Lock	Press Scroll Lock key twice quickly
Double Click Num Lock	Press Num Lock key twice quickly
Double Click Caps Lock	Press Caps Lock key twice quickly
Double Click Left Alt key	Press the left Alt key twice quickly
Double Click Left Shift key	Press the left Shift key twice quickly
Double Click Left Ctrl key	Press the left Ctrl key twice quickly

4. Set the Video Switching Delay from between 0 - 5 seconds, if necessary. Generally 0 is used unless more time is needed (certain monitors require more time to switch the video).

5. If you would like to use the power save feature:

   a. Select the Power Save Mode checkbox.

   b. Set the amount of time (in minutes) in which Power Save Mode will be initiated.

6. Choose the resolution for the Dominion KX II Local Console from the drop-down list:

   - 800x600
   - 1024x768
   - 1280x1024

7. Choose the refresh rate from the drop-down list:

   - 60 Hz
   - 75 Hz

8. Choose the type of local user authentication:

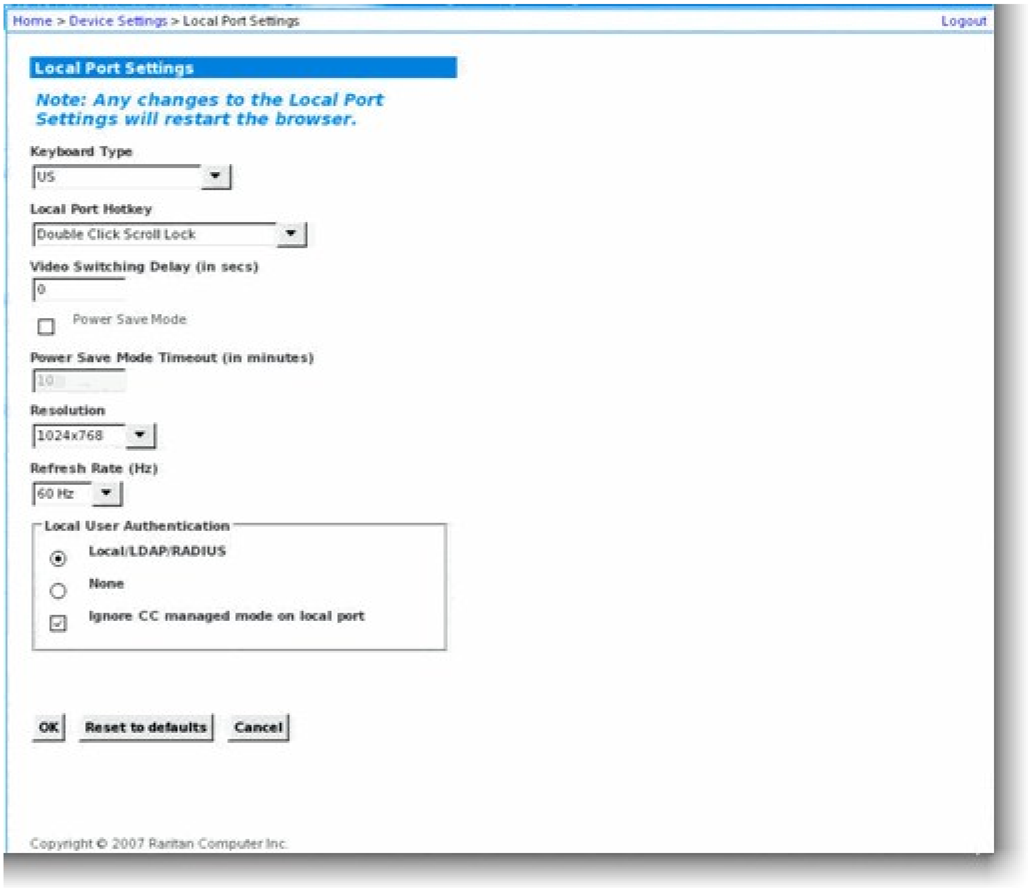
   - Local/LDAP/RADIUS. This is the recommended option. For more information about authentication, refer to ***Remote Authentication*** (on page 20).

- None. There is no authentication for Local Console access. This option is recommended for secure environments only.

9. Select the "Ignore CC managed mode on local port" checkbox if you would like local user access to the Dominion KX II even when the device is under CC-SG management.

Note: If you initially choose to ignore CC Manage mode on the local port but later want local port access, you will have to remove the device from under CC-SG management (from within CC-SG). You will then be able to check this checkbox.

10. Click OK.



Home > Device Settings > Local Port Settings

Logout

Local Port Settings

Note: Any changes to the Local Port Settings will restart the browser.

Keyboard Type: US

Local Port Hotkey: Double Click Scroll Lock

Video Switching Delay (in secs): 0

□ Power Save Mode

Power Save Mode Timeout (in minutes): 10

Resolution: 1024x768

Refresh Rate (Hz): 60 Hz

Local User Authentication

● Local/LDAP/RADIUS

○ None

☑ Ignore CC managed mode on local port

Copyright © 2007 Raritan Computer Inc.

➢ *To reset back to defaults:*

- Click Reset to Defaults.

Dominion KX II Local Console Factory Reset

Note: This feature is available only on the Dominion KX II Local Console.

The Dominion KX II offers several types of reset modes from the Local Console user interface.

Note: It is recommended that you save the audit log prior to performing a factory reset. The audit log is deleted when a factory reset is performed and the reset event is not logged in the audit log. For more information about saving the audit log, refer to ***Audit Log*** (on page 258).

➢ ***To perform a factory reset:***

1. Choose Maintenance > Factory Reset. The Factory Reset page opens.
2. Choose the appropriate reset option.

- Full Factory Reset - Removes the entire configuration and resets the unit completely to the factory defaults. Note that any management associations with CommandCenter will be broken. Because of the complete nature of this reset, you will be prompted to confirm the factory reset.
- Network Parameter Reset - Resets the network parameters of the unit back to the default values (click Device Settings > Network Settings to access this information):
  - IP auto configuration
  - IP address
  - Subnet mask
  - Gateway IP address
  - Primary DNS server IP address
  - Secondary DNS server IP address
  - Discovery port
  - Bandwidth limit
  - LAN interface speed & duplex
  - Enable automatic failover
  - Ping interval (seconds)
  - Timeout (seconds)

1. Click Reset to continue. You will be prompted to confirm the factory reset because all network settings will be permanently lost.

2. Click the Really Reset button to proceed. Upon completion, the Dominion KX II unit is automatically restarted.

Resetting the Dominion KX II Using the Reset Button

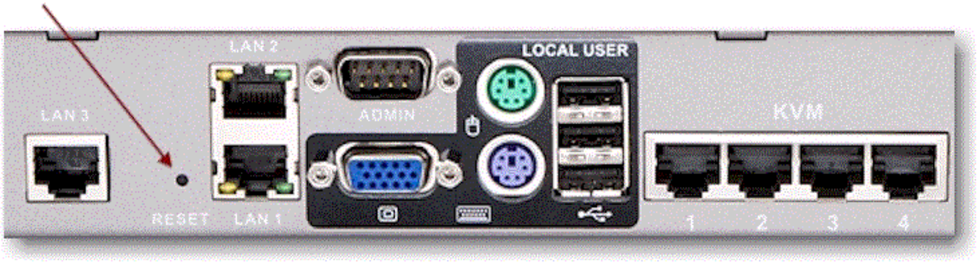
At the back of the Dominion KX II, there is a Reset button. It is recessed to prevent accidental presses (you will need a pointed object to use this button).

The actions that are performed when the Reset button is pressed are defined in the graphical user interface. Refer to ***Encryption & Share*** (on page 253) for more information.

Note: It is recommended that you save the audit log prior to performing a factory reset. The audit log is deleted when a factory reset is performed and the reset event is not logged on the audit log. For more information about saving the audit log, refer to ***Audit Log*** (on page 258).

➢ ***To reset the device:***

1. Power off the Dominion KX II device.
2. Use a pointed object to press and hold the Reset button.
3. While continuing to hold the Reset button, power the Dominion KX II device back on.
4. Continue holding the Reset button for 5-10 seconds. Once the device has been reset, two short beeps signal its completion.



Appendix A Specifications

In This Chapter

Supported Video Resolutions

Ensure that each target server's video resolution and refresh rate are supported by Dominion KX II and that the signal is noninterlaced.

Video resolution and cable length are important factors in the ability to obtain mouse synchronization. Refer to ***Target Server Connection Distance and Video Resolution*** (on page 299) for more information.

Dominion KX II supports these resolutions:

Resolutions		
640x350 @70 Hz	720x400 @85 Hz	1024x768 @90 Hz
640x350 @85 Hz	800x600 @56 Hz	1024x768 @100 Hz
640x400 @56 Hz	800x600 @60 Hz	1152x864 @60 Hz
640x400 @84 Hz	800x600 @70 Hz	1152x864 @70 Hz
640x400 @85 Hz	800x600 @72 Hz	1152x864 @75 Hz
640x480 @60 Hz	800x600 @75 Hz	1152x864 @85 Hz
640x480 @66.6 Hz	800x600 @85 Hz	1152x870 @75.1 Hz
640x480 @72 Hz	800x600 @90 Hz	1152x900 @66 Hz
640x480 @75 Hz	800x600 @100 Hz	1152x900 @76 Hz
640x480 @85 Hz	832x624 @75.1 Hz	1280x960 @60 Hz

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

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

Supported Keyboard Languages

The Dominion KX II provides keyboard support for the languages listed in the following table.

Note: You can use the keyboard for Chinese, Japanese, and Korean for display only; local language input is not supported at this time for Dominion KX II Local Console functions. For more information about non-US keyboards, see ***Informational Notes*** (on page 311).

Language	Regions	Keyboard layout
US English	United States of America and most of English-speaking countries: for example, Canada, Australia, and New Zealand.	US Keyboard layout.
US English International	United States of America and most of English-speaking countries: for example, Netherlands	US Keyboard layout.
UK English	United Kingdom	UK layout keyboard
Chinese Traditional	Hong Kong S. A. R., Republic of China (Taiwan)	Chinese Traditional
Chinese Simplified	Mainland of the People's Republic of China	Chinese Simplified
Korean	South Korea	Dubeolsik Hangul
Japanese	Japan	JIS Keyboard

Language	Regions	Keyboard layout
French	France	French (AZERTY) layout keyboard.
German	Germany and Austria	German keyboard (QWERTZ layout).
Belgium	Belgium	Belgian
Norway	Norway	Norwegian
Denmark	Denmark	Danish
Sweden	Sweden	Swedish

Supported Operating Systems (Clients)

The following operating systems are supported on the Virtual KVM Client™ and Multi-Platform Client (MPC):

Client OS	Virtual media (VM) support on client
Windows XP®	Yes
Windows 2000 SP4®	Yes
Windows Vista®	Yes
Red Hat® Linux 9.0	Yes. Locally held ISO image, Remote File Server mounting directly from Dominion KX II
Red Hat Enterprise Workstation 3.0 and 4.0	Yes. Locally held ISO image, Remote File Server mounting directly from Dominion KX II
SUSE Linux Professional 9.2 and 10	Yes. Locally held ISO image, Remote File Server mounting directly from Dominion KX II
Fedora™ Core 5 and above	Yes. Locally held ISO image, Remote File Server mounting directly from Dominion KX II
Mac®	No
Solaris	No

Supported Browsers

Dominion KX II supports the following browsers:

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

Supported Operating Systems and CIMs (Target Servers)

In addition to the new Dominion KX II D2CIMs, most Paragon® and Dominion KX I CIMs are supported. The following table displays the supported target server operating systems, CIMs, virtual media, and mouse modes:

Note: D2CIM-VUSB is not supported on Sun (Solaris) targets.

Target server	Supported CIMs			VM	Mouse modes		
	Paragon CIMs	Dominion KX I DCIMs	Dominion KX II D2CIMs		AM	IM	SM
Windows XP Windows 2000 Windows 2000 Server Windows 2003 Server Windows Vista	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB and D2CIM-DVUSB	✓	✓	✓	✓
Red Hat Linux 9.0 Red Hat Enterprise Workstation 3.0 and 4.0	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB (excluding Red Hat Enterprise Workstation 3.0)	✓			✓

Supported Operating Systems and CIMs (Target Servers)

Target server	Supported CIMs			VM	Mouse modes		
	Paragon CIMs	Dominion KX I DCIMs	Dominion KX II D2CIMs		AM	IM	SM
SUSE Linux Professional 9.2 and 10	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB and D2CIM-DVUSB	✓			✓
Fedora Core 3 and above	P2CIM-PS2 P2CIM-AUSB UKVMPD UUSBPD	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Mac OS	P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓		
All Solaris OSs supported in Dominion KX I	P2CIM-SUN P2CIM-SUSB	DCIM-SUN DCIM-SUSB DCIM-USB G2					✓
IBM AIX	P2CIM-PS2 P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
HP UX	P2CIM-PS2 P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
Remote Power Strips			D2CIM-PWR				
Serial Devices	P2CIM-SER						

Legend	
VM	Virtual Media (D2CIM-VUSB and D2CIM-DVUSB only)
AM	Absolute Mouse Synchronization (D2CIM-VUSB and D2CIM-DVUSB only)
IM	Intelligent Mouse Mode
SM	Standard Mouse Mode
✓	Supported

Note: The DCIM-USB G2 provides a small slide switch on the back of the CIM. Move the switch to P for PC-based USB target servers; move the switch to S for Sun USB target servers.
A new switch position takes effect only after the CIM is power-cycled. To power-cycle the CIM, remove the USB connector from the target server and plug it back in a few seconds later.

Environmental Requirements

Operating	
Temperature	0°C- 40°C (32°F - 104°F)
Humidity	20% - 85% RH
Altitude	N/A
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A
Non-Operating	
Temperature	0°C- 50°C (32°F - 122°F)
Humidity	10% - 90% RH
Altitude	N/A
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A

Physical Specifications

Part number	Line item description	Weight	Product dimensions (WxDxH)	Shipping weight	Shipping dimensions (WxDxH)	UPC code	Power
DKX2-108	8-Port Dominion KX II with 1-user Network Access and Local Port; Virtual Media, Dual Power	8.58 lbs; 3.9kg	1.75" x 17.32" x 11.4" 44mm x 439mm x 290mm	14.3 lbs; 6.5 kg	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	785813624109	Dual Power 100/240 V 50/60 Hz 0.6A 61.3 Watts
DKX2-116	16-Port Dominion KX II with 1-user Network Access and Local Port; Virtual Media, Dual Power	8.65 lbs; 3.9kg	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	14.85 lbs; 6.7 kg	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	785813624055	Dual Power 100/240 V 50/60 Hz 0.6A 25.4 Watts
DKX2-132	32-Port Dominion KX II with 1-user Network Access and Local Port; Virtual Media, Dual Power	9.0 lbs; 4.1kg	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	14.9 lbs; 6.8 kg	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	785813624079	Dual Power 100/240 V 50/60 Hz 0.6A 26 Watts
DKX2-216	16-Port Dominion KX II with 2-user Network Access and Local Port; Virtual Media, Dual Power	8.65 lbs; 3.9 kg	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	14.49 lbs; 6.6 kg	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	785813624086	Dual Power 100/240 V 50/60 Hz 0.6A 26.3 Watts

Part number	Line item description	Weight	Product dimensions (WxDxH)	Shipping weight	Shipping dimensions (WxDxH)	UPC code	Power
DKX2-232	32-Port Dominion KX II with 2-user Network Access and Local Port; Virtual Media, Dual Power	9.0 lbs; 4.1 kg	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	14.9 lbs; 6.8 kg	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	785813625021	Dual Power 100/240 V 50/60 Hz (optimal 47 - 63 Hz) 0.6A 27 Watts
DKX2-416	16-Port Dominion KX II with 4-user Network Access and Local Port; Virtual Media, Dual Power	9.04 lbs; 4.1 kg	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	14.94 lbs; 6.8 kg	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	785813625359	Dual Power 100/240 V 50/60 Hz 1A 62 Watts
DKX2-432	32-Port Dominion KX II with 4-user Network Access and Local Port; Virtual Media, Dual Power	9.48 lbs; 4.3 kg	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	15.38 lbs; 7.0 kg	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	785813625380	Dual Power 100/240 V 50/60 Hz 1A 64 Watts

Computer Interface Modules (CIMs)

Part number	Line item description	Product weight	Product dimensions (WxDxH)	Shipping weight	Shipping dimensions (WxDxH)	UPC code
D2CIM-VUSB	Dominion KX II Computer Interface Module [USB Port with Virtual Media]	0.2 lbs	1.3" x 3.0" x 0.6"	0.2 lbs	7.2" x 9" x 0.6"	785813332004

Computer Interface Modules (CIMs)

Part number	Line item description	Product weight	Product dimensions (WxDxH)	Shipping weight	Shipping dimensions (WxDxH)	UPC code
DCIM-PS2	Dominion KX I & II Computer Interface Module [PS/2 Port]	0.2 lbs	1.3" x 3.0" x 0.6"	0.2 lbs	7.2" x 9" x 0.6"	785813338532
DCIM-USB	Dominion KX I & II Computer Interface Module [USB Port]	0.2 lbs	1.3" x 3.0" x 0.6"	0.2 lbs	7.2" x 9" x 0.6"	785813338518
DCIM-SUSB	Dominion KX I & II Computer Interface Module [USB Port for Sun]	0.2 lbs	1.3" x 3.0" x 0.6"	0.2 lbs	7.2" x 9" x 0.6"	785813338556
DCIM-USBG2	Dominion KX I & II Computer Interface Module [USB and Sun USB Port] G2 CIM	0.2 lbs	1.3” x 3.0” x 0.6”	0.2 lbs	7.2” x 9” x 0.6	785813338884
DCIM-SUN	Dominion KX I & II Computer Interface Module [Sun Port, HD15 Video]	0.2 lbs	1.3" x 3.0" x 0.6"	0.2 lbs	7.2" x 9" x 0.6"	785813338549
D2CIM-PWR	Dominion KX II Computer Interface Module for Remote Power strips	0.2 lbs	1.3" x 3.0" x 0.6"	0.2 lbs	7.2" x 9" x 0.6"	785813332011
D2CIM-VUSB-32PAC	Bulk pack of 32 D2CIM-VUSB	6.4 lb	(1.3" x 3.0" x 0.6")*32	8.01 lb	21.65"x12.20"x 4.33"	785813332028
D2CIM-VUSB -64PAC	Bulk pack of 64 D2CIM-VUSB	12.8 lb	(1.3" x 3.0" x 0.6")*64	18.13 lb	22.64"x9.45"x12.99"	785813332035

Part number	Line item description	Product weight	Product dimensions (WxDxH)	Shipping weight	Shipping dimensions (WxDxH)	UPC code
D2CIM-DVUSB	Dominion KX II Computer Interface Module [Dual USB Port with Virtual Media]	0.23 lbs, 105g	3.53″x1.68″x.76″ 89.7x42.7x19.3 (mm)	.25 lbs, 112.5g	3.9″x5.7″x 1.0″ 100*145*27 (mm)	785813339508
D2CIM-DVUSB-32PAC	Bulk pack of 32 D2CIM-DVUSB	10.1 lbs, 4.6kg	21.9″x12.2″x4.3″ 555x310x110 (mm)	10.1 lbs, 4.6kg	21.9″x12.2″x4.3″ 555x310x110 (mm)	785813332080
D2CIM-DVUSB - 64PAC	Bulk pack of 64 D2CIM-DVUSB	22.5 lbs, 10.2 kg	9.4″x22.6″x13.0″ 240x575x330 (mm)	22.5 lbs, 10.2 kg	9.4″x22.6″x13.0″ 240*575*330 (mm)	785813332097

Remote Connection

Remote connection	Details
Network	10BASE-T, 100BASE-T, and 1000BASE-T (Gigabit) Ethernet
Protocols	TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

TCP and UDP Ports Used

TCP and UDP Ports Used

Port	Description
HTTP, Port 80	All requests received by Dominion KX II via HTTP (port 80) are automatically forwarded to HTTPS for complete security. Dominion KX II responds to Port 80 for user convenience, relieving users from having to explicitly type *https://* in the URL field to access Dominion KX II, but while still preserving complete security.
HTTPS, Port 443	This port is used for a number of purposes, including the web server for the HTML client, the download of client software (MPC/KVC) onto the client's host, and the transfer of KVM and Virtual Media data streams to the client.
Dominion KX II (Raritan KVM-over-IP) Protocol, Configurable Port 5000	This port is used to discover other Dominion devices and for communication between Raritan devices and systems, including CC-SG. By default, this is set to Port 5000, but you may configure it to use any TCP port not currently in use. For details on how to configure this setting, refer to ***Network Settings*** (on page 219).
SNTP (Time Server) on Configurable UDP Port 123	Dominion KX II offers the optional capability to synchronize its internal clock to a central time server. This function requires the use of UDP Port 123 (the standard for SNTP), but can also be configured to use any port of your designation. **Optional**
LDAP/LDAPS on Configurable Ports 389 or 636	If Dominion KX II is configured to remotely authenticate user logins via the LDAP/LDAPS protocol, ports 389 or 636 will be used, but the system can also be configured to use any port of your designation. **Optional**
RADIUS on Configurable Port 1812	If Dominion KX II is configured to remotely authenticate user logins via the RADIUS protocol, either port 1812 will be used, but the system can also be configured to use any port of your designation. **Optional**
RADIUS Accounting on Configurable Port 1813	If Dominion KX II is configured to remotely authenticate user logins via the RADIUS protocol, and also employs RADIUS accounting for event logging, port 1813 or an additional port of your designation will be used to transfer log notifications.
SYSLOG on Configurable UDP Port 514	If Dominion KX II is configured to send messages to a Syslog server, then the indicated port(s) will be used for communication - uses UDP Port 514.
SNMP Default UDP Ports	Port 161 is used for inbound/outbound read/write SNMP access and port 162 is used for outbound traffic for SNMP traps. **Optional**
TCP Port 21	Port 21 is used for the KX II command line interface (when you are working with Raritan Technical Support).

Target Server Connection Distance and Video Resolution

The maximum supported distance is a function of many factors including the type/quality of Cat 5 cable, server type and manufacturer, video driver and monitor, environmental conditions, and user expectations. The following table summarizes the maximum target server distance for various video resolutions and refresh rates:

Video resolution	Refresh rate	Maximum distance
1600x1200	60	50 ft (15 m)
1280x1024	60	100 ft (30 m)
1024x768	60	150 ft (45 m)

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

Refer to the ***Supported Video Resolutions*** (on page 288) for the video resolutions supported by Dominion KX II.

Network Speed Settings

		Dominion KX II network speed setting					
Network switch port setting		Auto	1000/Full	100/Full	100/Half	10/Full	10/Half
	Auto	Highest Available Speed	1000/Full	Dominion KX II: 100/Full Switch: 100/Half	100/Half	Dominion KX II: 10/Full Switch: 10/Half	10/Half
	1000/Full	1000/Full	1000/Full	No Communication	No Communication	No Communication	No Communication
	100/Full	Dominion KX II: 100/Half Switch: 100/Full	Dominion KX II: 100/Half Switch: 100/Full	100/Full	Dominion KX II: 100/Half Switch: 100/Full	No Communication	No Communication
	100/Half	100/Half	100/Half	Dominion KX II: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
	10/Full	Dominion KX II: 10/Half Switch: 10/Full	No Communication	No Communication	No Communication	10/Full	Dominion KX II: 10/Half Switch: 10/Full
	10/Half	10/Half	No Communication	No Communication	No Communication	Dominion KX II: 10/Full Switch: 10/Half	10/Half

Legend:

□ Does not function, as expected

🟩	Supported
🟦	Functions; not recommended
🟥	NOT supported by Ethernet specification; product will communicate, but collisions will occur
□	Per Ethernet specification, these should be "no communication", however, note that the Dominion KX II behavior deviates from expected behavior

Note: For reliable network communication, configure the Dominion KX II and the LAN switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX II and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.

Appendix B Updating the LDAP Schema

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

In This Chapter

Returning User Group Information

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

From LDAP

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

rciusergroup	attribute type: string

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

From Microsoft Active Directory

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

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

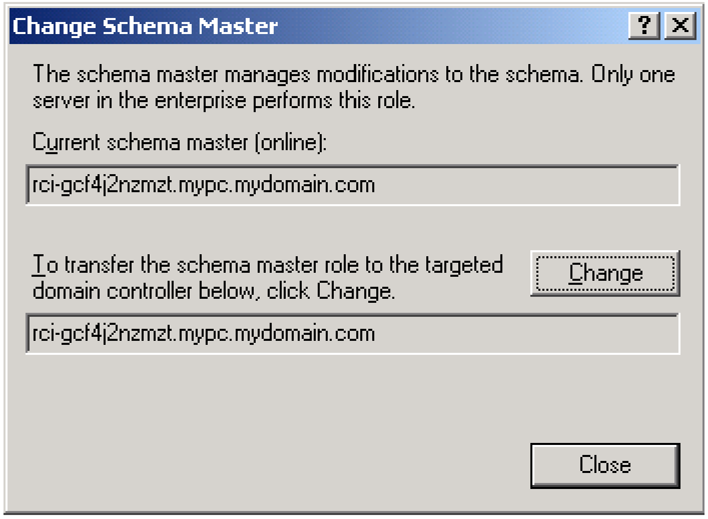
1. Install the schema plug-in for Active Directory. Refer to Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

Setting the Registry to Permit Write Operations to the Schema

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

➤ ***To permit write operations to the schema:***

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



The schema master manages modifications to the schema. Only one server in the enterprise performs this role.

Current schema master (online):

rci-gcf4j2nzmzt.mypc.mydomain.com

To transfer the schema master role to the targeted domain controller below, click Change.

rci-gcf4j2nzmzt.mypc.mydomain.com

2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**

3. Click OK.

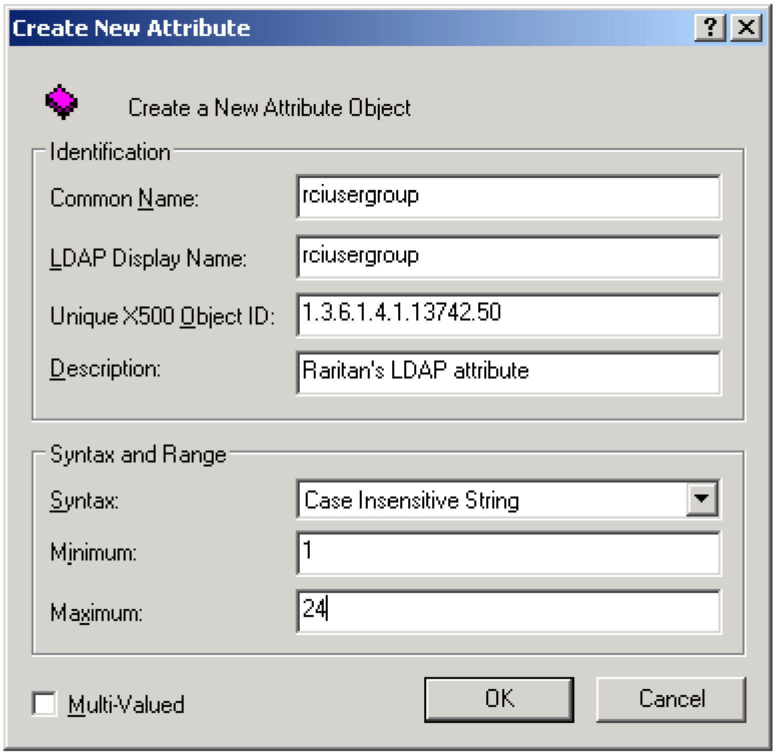
Creating a New Attribute

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

1. Click the + symbol before Active Directory Schema in the left pane of the window.

2. Right-click Attributes in the left pane.

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



Create New Attribute

Create a New Attribute Object

Identification

Common Name: rciusergroup

LDAP Display Name: rciusergroup

Unique X500 Object ID: 1.3.6.1.4.1.13742.50

Description: Raritan's LDAP attribute

Syntax and Range

Syntax: Case Insensitive String

Minimum: 1

Maximum: 24

□ Multi-Valued

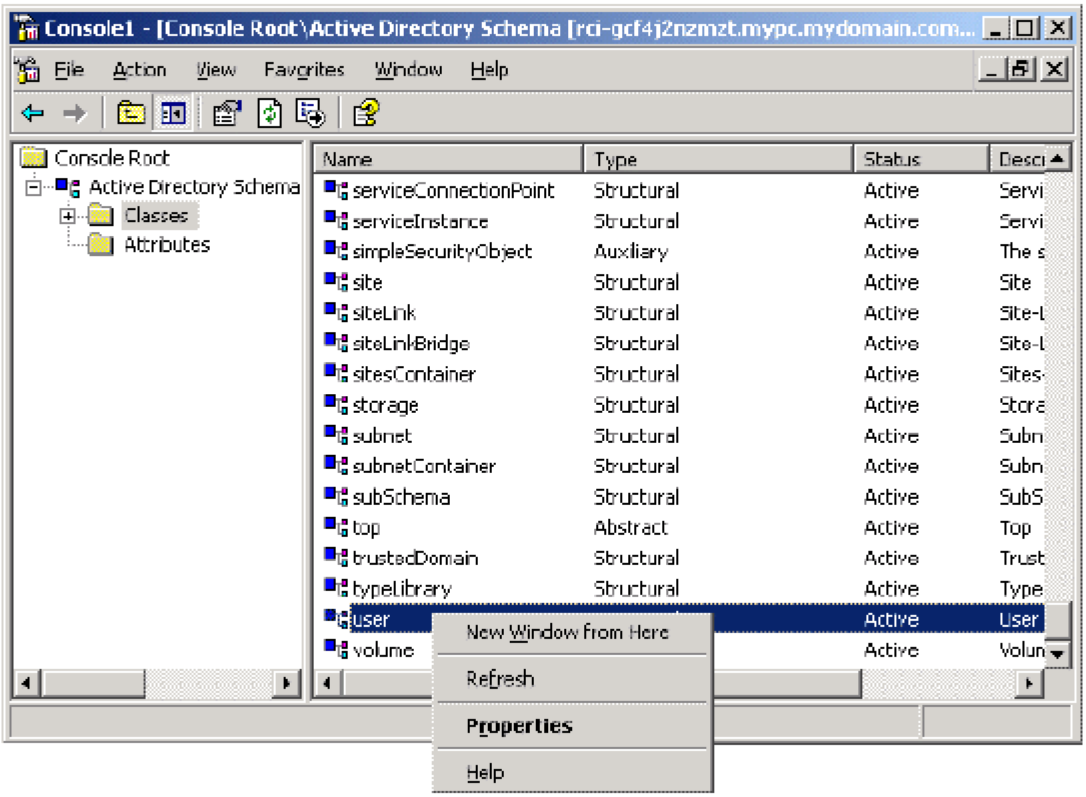
4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String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

Adding Attributes to the Class

➢ ***To add attributes to the class:***

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

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



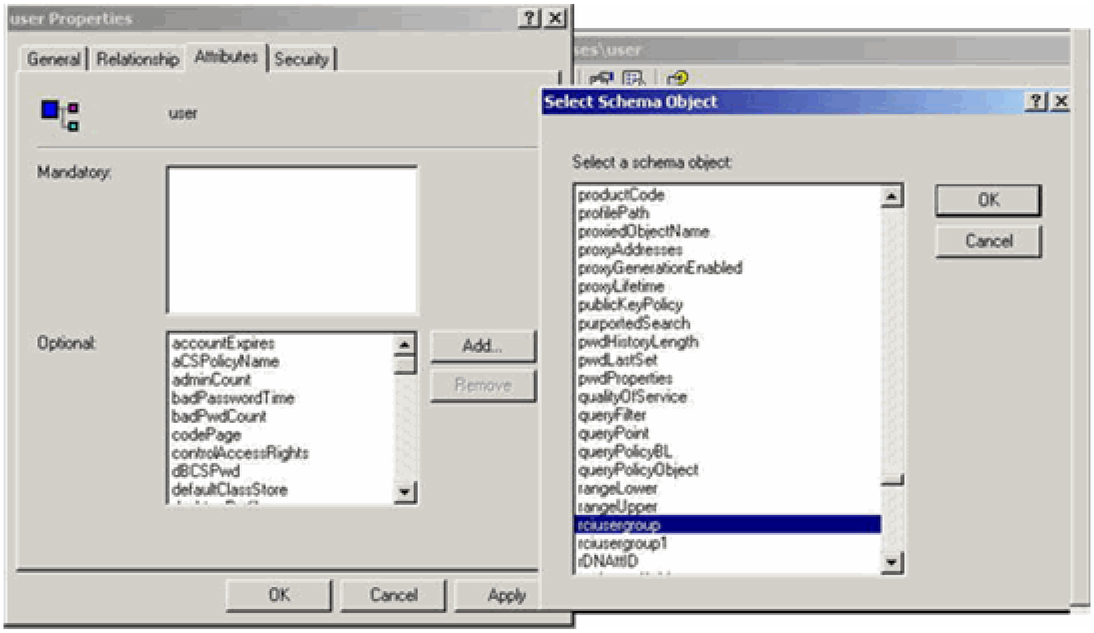
Name	Type	Status	Descri
serviceConnectionPoint	Structural	Active	Servi
serviceInstance	Structural	Active	Servi
simpleSecurityObject	Auxiliary	Active	The s
site	Structural	Active	Site
siteLink	Structural	Active	Site-L
siteLinkBridge	Structural	Active	Site-L
sitesContainer	Structural	Active	Sites
storage	Structural	Active	Stora
subnet	Structural	Active	Subn
subnetContainer	Structural	Active	Subn
subSchema	Structural	Active	SubS
top	Abstract	Active	Top
trustedDomain	Structural	Active	Trust
typeLibrary	Structural	Active	Type
user		Active	User
volume		Active	Volun

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

4. Click the Attributes tab to open it.

5. Click Add.

6. Choose rciusergroup from the Select Schema Object list.



7. Click OK in the Select Schema Object dialog.

8. Click OK in the User Properties dialog.

Updating the Schema Cache

➢ ***To update the schema cache:***

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

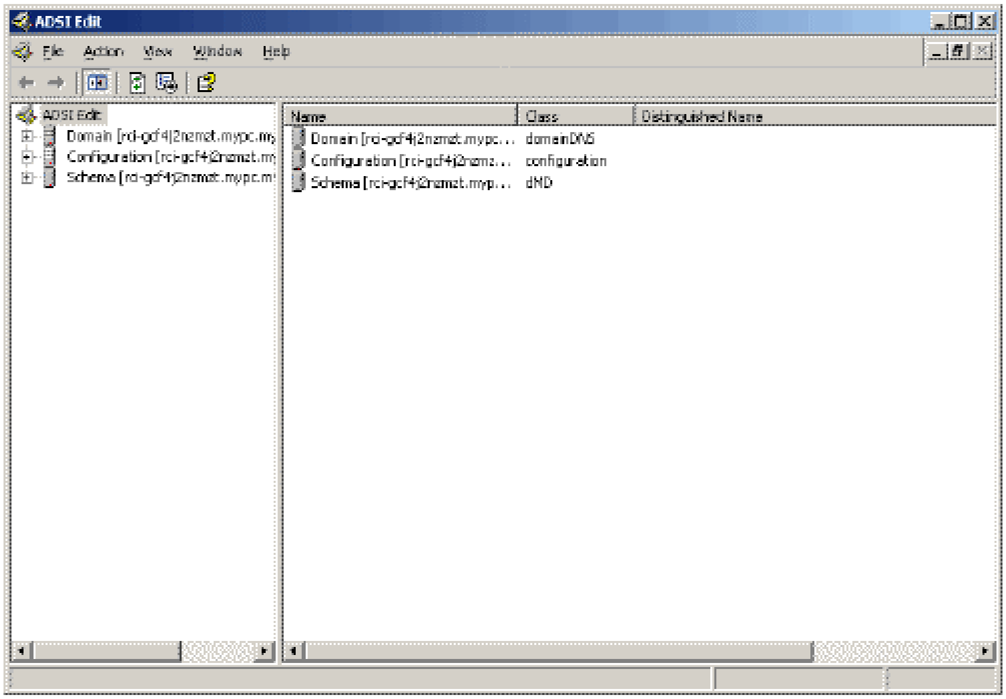
2. Minimize the Active Directory Schema MMC (Microsoft Management Console) console.

Editing rciusergroup Attributes for User Members

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

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

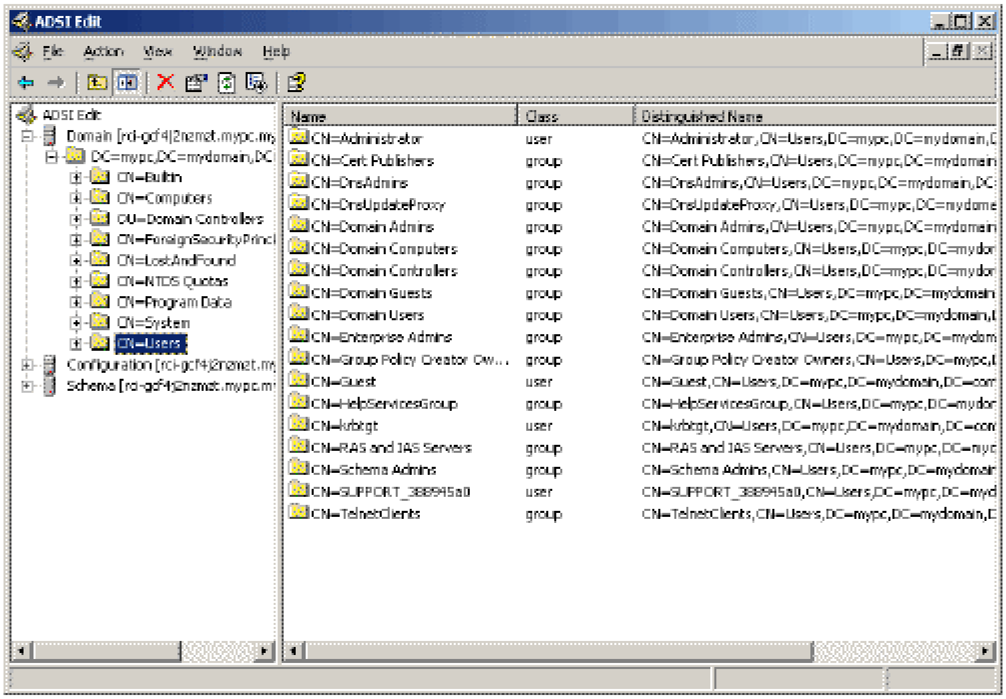
1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.
3. Go to the directory where the support tools were installed.
4. Run adsiedit.msc. The ADSI Edit window opens.


ADSI Edit
File
Action
View
Window
Help
ADSI Edit
Domain [rci-gcf4j2nzmzt.mypc.m
Configuration [rci-gcf4j2nzmzt.m
Schema [rci-gcf4j2nzmzt.mypc.m

Name	Class	Distinguished Name
Domain [rci-gcf4j2nzmzt.mypc...	domainDNS	
Configuration [rci-gcf4j2nzmz...	configuration	
Schema [rci-gcf4j2nzmzt.myp...	dMD	

5. Open the Domain.

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

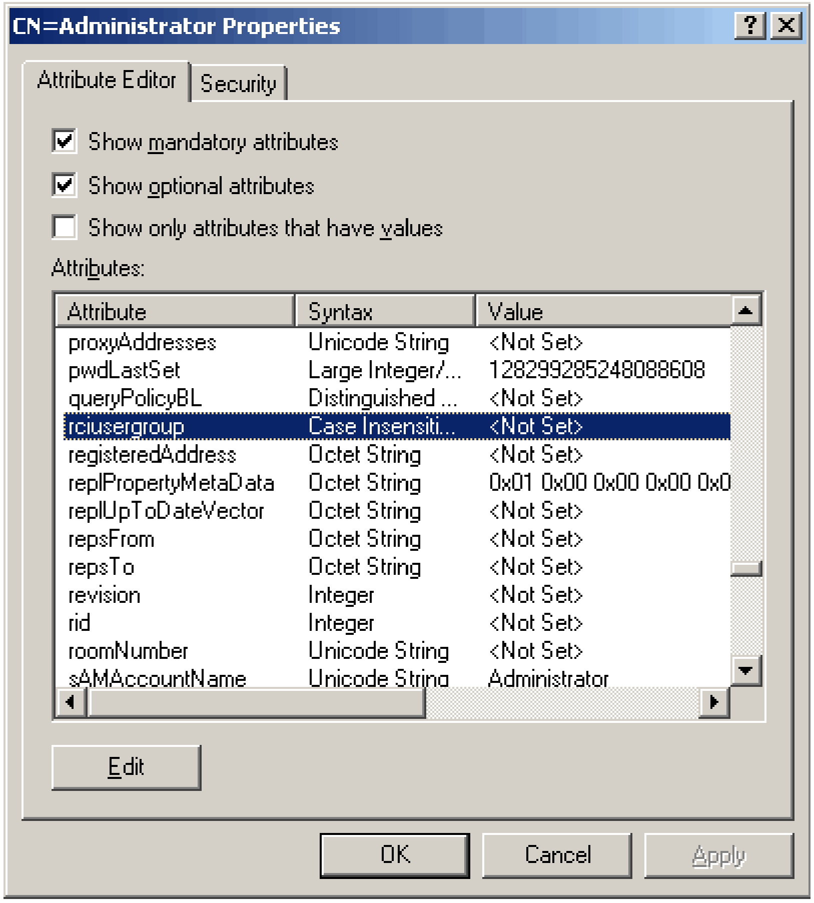


Name	Class	Distinguished Name
CN=Administrator	user	CN=Administrator,CN=Users,DC=mypc,DC=mydomain,[
CN=Cert Publishers	group	CN=Cert Publishers,CN=Users,DC=mypc,DC=mydomain
CN=DnsAdmins	group	CN=DnsAdmins,CN=Users,DC=mypc,DC=mydomain,DC:
CN=DnsUpdateProxy	group	CN=DnsUpdateProxy,CN=Users,DC=mypc,DC=mydome
CN=Domain Admins	group	CN=Domain Admins,CN=Users,DC=mypc,DC=mydomain
CN=Domain Computers	group	CN=Domain Computers,CN=Users,DC=mypc,DC=mydor
CN=Domain Controllers	group	CN=Domain Controllers,CN=Users,DC=mypc,DC=mydor
CN=Domain Guests	group	CN=Domain Guests,CN=Users,DC=mypc,DC=mydomain
CN=Domain Users	group	CN=Domain Users,CN=Users,DC=mypc,DC=mydomain,I
CN=Enterprise Admins	group	CN=Enterprise Admins,CN=Users,DC=mypc,DC=mydom
CN=Group Policy Creator Ow...	group	CN=Group Policy Creator Owners,CN=Users,DC=mypc,I
CN=Guest	user	CN=Guest,CN=Users,DC=mypc,DC=mydomain,DC=cor
CN=HelpServicesGroup	group	CN=HelpServicesGroup,CN=Users,DC=mypc,DC=mydor
CN=krbtgt	user	CN=krbtgt,CN=Users,DC=mypc,DC=mydomain,DC=cor
CN=RAS and IAS Servers	group	CN=RAS and IAS Servers,CN=Users,DC=mypc,DC=myc
CN=Schema Admins	group	CN=Schema Admins,CN=Users,DC=mypc,DC=mydomair
CN=SUPPORT_388945a0	user	CN=SUPPORT_388945a0,CN=Users,DC=mypc,DC=myd
CN=TelnetClients	group	CN=TelnetClients,CN=Users,DC=mypc,DC=mydomain,D

7. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.

8. Click the Attribute Editor tab if it is not already open.

9. Choose rciusergroup from the Attributes list.



CN=Administrator Properties

Attribute Editor | Security

☑ Show mandatory attributes

☑ Show optional attributes

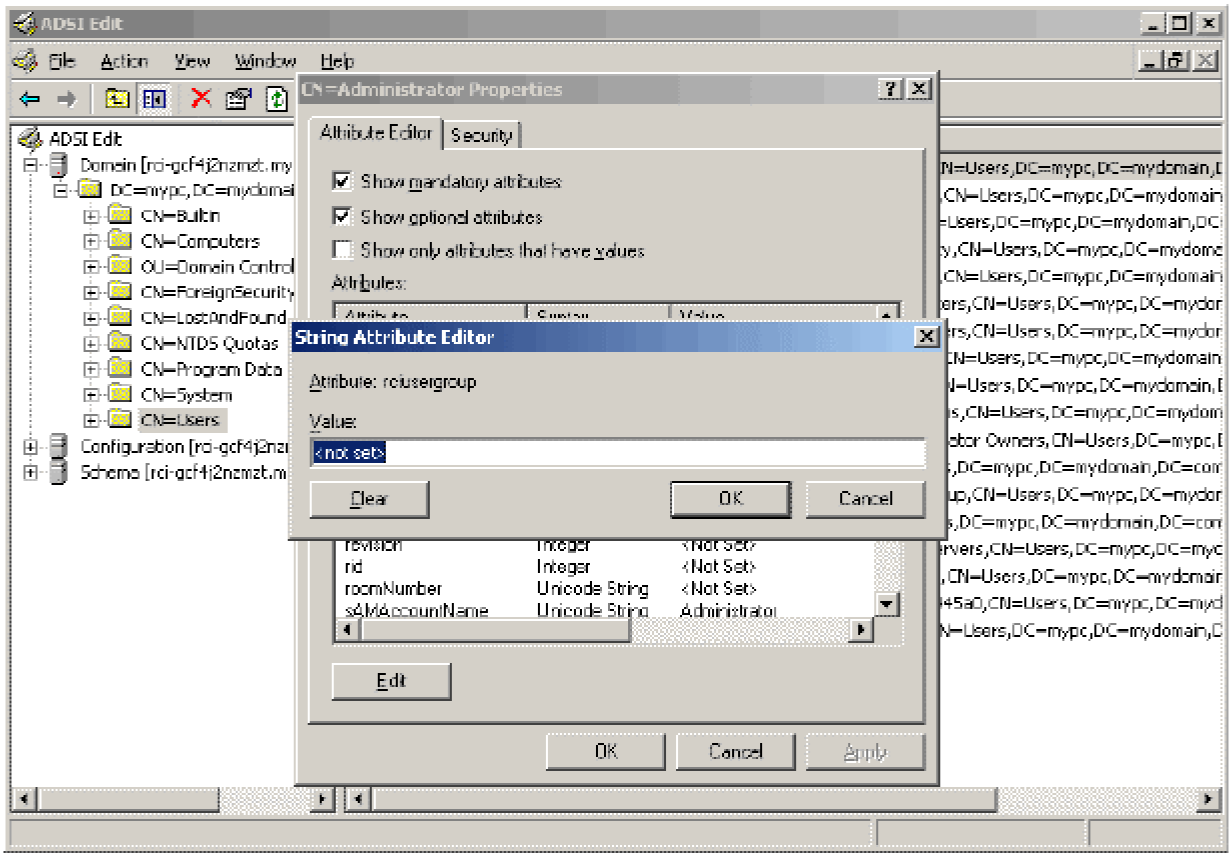
☐ Show only attributes that have values

Attributes:

Attribute	Syntax	Value
proxyAddresses	Unicode String	<Not Set>
pwdLastSet	Large Integer/...	128299285248088608
queryPolicyBL	Distinguished ...	<Not Set>
rciusergroup	Case Insensiti...	<Not Set>
registeredAddress	Octet String	<Not Set>
replPropertyMetaData	Octet String	0x01 0x00 0x00 0x00 0x0
replUpToDateVector	Octet String	<Not Set>
repsFrom	Octet String	<Not Set>
repsTo	Octet String	<Not Set>
revision	Integer	<Not Set>
rid	Integer	<Not Set>
roomNumber	Unicode String	<Not Set>
sAMAccountName	Unicode String	Administrator

Editing rciusergroup Attributes for User Members

10. Click Edit. The String Attribute Editor dialog appears.



☑ Show mandatory attributes

☑ Show optional attributes

☐ Show only attributes that have values

Attributes:

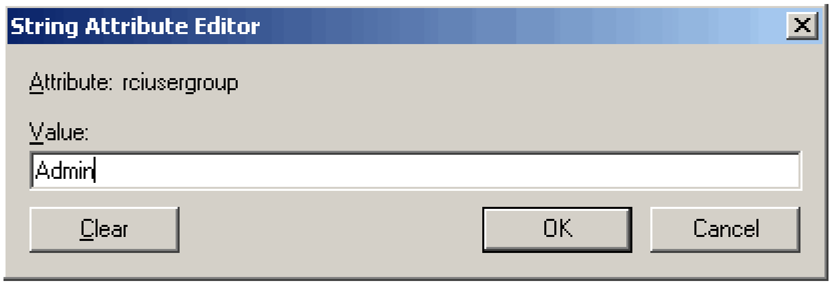
Attribute	Syntax	Value
revision	Integer	<Not Set>
rid	Integer	<Not Set>
roomNumber	Unicode String	<Not Set>
sAMAccountName	Unicode String	Administrator

String Attribute Editor

Attribute: rciusergroup

Value: <not set>

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



String Attribute Editor

Attribute: rciusergroup

Value: Admin

12. Click OK.

Appendix C Informational Notes

In This Chapter

Overview

This section includes important notes on Dominion KX II usage. Future updates will be documented and available online through the Help - User Guide link in the Dominion KX II Remote Console interface.

Java Runtime Environment (JRE)

Important: It is recommended that you disable Java caching and clear the Java cache. Refer to your Java documentation or MPC Requirements and Installation Instructions.

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

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

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

Keyboards

Non-US Keyboards

French Keyboard

Caret Symbol (Linux Clients Only)

The Virtual KVM Client and the Multi-Platform Client (MPC) do not process the key combination of Alt Gr + 9 as the caret symbol (^) when using French keyboards with Linux clients.

➢ ***To obtain the caret symbol:***

From a French keyboard, press the ^ key (to the right of the P key), then immediately press the space bar.

Alternatively, create a macro consisting of the following commands:

1. Press Right Alt
2. Press 9.
3. Release 9.
4. Release Right Alt.

Note: These procedures do not apply to the circumflex accent (above vowels). In all cases, the ^ key (to the right of the P key) works on French keyboards to create the circumflex accent when used in combination with another character.

Accent Symbol (Windows XP Clients Only)

From the Virtual KVM Client and the Multi-Platform Client, the key combination of Alt Gr + 7 results in the accented character displaying twice when using French keyboards with Windows XP clients.

Note: This does not occur with Linux clients.

Numeric Keypad

From the Virtual KVM Client and the Multi-Platform Client, the numeric keypad symbols display as follows when using a French keyboard:

Numeric keypad symbol	Displays as
/	;
.	;

Tilde Symbol

From the Virtual KVM Client and the Multi-Platform Client, the key combination of Alt Gr + 2 does not produce the tilde (~) symbol when using a French keyboard.

➢ ***To obtain the tilde symbol:***

Create a macro consisting of the following commands:

- Press right Alt.
- Press 2.
- Release 2.
- Release right Alt.

Key Combinations and the Java Runtime Environment (JRE)

Because of a limitation in the Java Runtime Environment (JRE), Fedora, Linux, and Solaris clients receive an invalid response from Alt Gr on UK English and US International language keyboards. Fedora, Linux, and Solaris do not pick up events for the Alt Gr key combination for Java 1.4.2 or 1.5. Java 1.6 appears to improve on this, although the keyPressed and keyReleased events for Alt Gr still identify it as an "unknown key code".

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

Keyboard Language Preference (Fedora Linux Clients)

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

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

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

When using a Hungarian keyboard from a Linux client, the Latin letter U with Double Acute and the Latin letter O with Double Acute work only with JRE 1.6.

There are several methods that can be used to set the keyboard language preference on Fedora Linux clients. The following method must be used in order for the keys to be mapped correctly from the Virtual KVM Client and the Multi-Platform Client (MPC).

➢ *To set the keyboard language using System Settings:*

1. From the toolbar, choose System > Preferences > Keyboard.
2. Open the Layouts tab.
3. Add or select the appropriate language.
4. Click Close.

➢ *To set the keyboard language using the Keyboard Indicator:*

1. Right-click the Task Bar and choose Add to Panel.
2. In the Add to Panel dialog, right-click the Keyboard Indicator and from the menu choose Open Keyboard Preferences.
3. In the Keyboard Preferences dialog, click the Layouts tab.
4. Add and remove languages as necessary.

Macintosh Keyboard

When a Macintosh is used as the client, the following keys on the Mac keyboard are not captured by the Java Runtime Environment (JRE):

- F9
- F10
- F11
- F14
- F15
- Volume Up
- Volume Down
- Mute
- Eject

As a result, the Virtual KVM Client and the Multi-Platform Client (MPC) are unable to process these keys from a Mac client's keyboard.

Special Sun Key Combinations

The following key combinations for Sun Microsystems server's special keys operate on the local port:

Sun key	Local port key combination
Again	Ctrl+ Alt +F2
Props	Ctrl + Alt +F3
Undo	Ctrl + Alt +F4
Stop A	Break a
Front	Ctrl + Alt + F5
Copy	Ctrl + Alt + F6
Open	Ctrl + Alt + F7
Find	Ctrl + Alt + F9
Cut	Ctrl + Alt + F10
Paste	Ctrl + Alt + F8
Mute	Ctrl + Alt + F12
Compose	Ctrl+ Alt + KPAD *

Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	No key combination
Power	No key combination

Mouse Pointer Synchronization (Fedora)

When connected in dual mouse mode to a target server running Fedora 7, the target and local mouse pointers may lose synchronization after some time.

➢ ***To resynchronize the mouse cursors:***

- Use the Synchronize Mouse option from the Virtual KVM Client.

The following table summarizes the Dominion KX II mouse modes, and whether or not these modes remain synchronized when accessing KVM target servers running Fedora:

Mouse mode	Fedora Core 5	Fedora Core 6
Absolute Mouse Synchronization	No	No
Intelligent Mouse Mode	No	Yes
Standard Mouse Mode	Yes	No

Resolving Fedora Core Focus

Using the Multi-Platform Client (MPC), occasionally there is an inability to log on to a Dominion KX II device or to access KVM target servers (Windows, SUSE, and so forth). In addition, the Ctrl+Alt+M key combination may not bring up the Keyboard Shortcut menu. This situation occurs with the following client configuration: Fedora Core 6 and Firefox 1.5 or 2.0.

Through testing, it has been determined that installation of libXp resolves window focusing issues with Fedora Core 6. Raritan has tested with libXp-1.0.0.8.i386.rpm; this resolved all of the keyboard focus and popup-menu problems.

Note: libXp is also required for the SeaMonkey (formerly Mozilla) browser to work with the Java plug in.

SUSE/VESA Video Modes

The SuSE X.org configuration tool SaX2 generates video modes using modeline entries in the X.org configuration file. These video modes do not correspond exactly with VESA video mode timing (even when a VESA monitor is selected). Dominion KX II, on the other hand, relies on exact VESA mode timing for proper synchronization. This disparity can result in black borders, missing sections of the picture, and noise.

➢ ***To configure the SUSE video display:***

1. The generated configuration file /etc/X11/xorg.conf includes a Monitor section with an option named UseModes. For example, UseModes "Modes[0]"
2. Either comment out this line (using #) or delete it completely.
3. Restart the X server.

With this change, the internal video mode timing from the X server will be used and will correspond exactly with the VESA video mode timing, resulting in the proper video display on the Dominion KX II.

USB Ports and Profiles

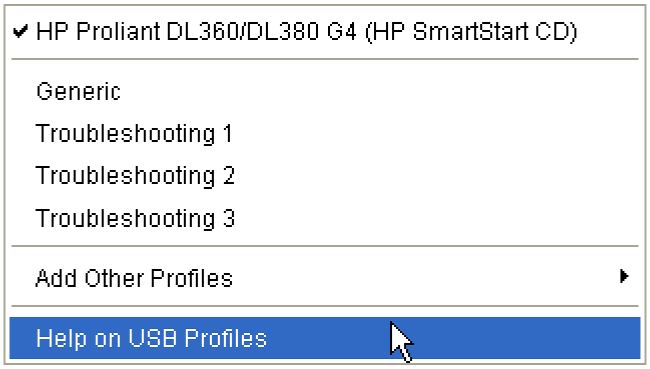
VM-CIMs and DL360 USB Ports

HP DL360 servers have one USB port on the back of the device and another on the front of the device. With the DL360, both ports cannot be used at the same time. Therefore, a dual VM-CIM cannot be used on DL360 servers.

However, as a workaround, a USB2 hub can be attached to the USB port on the back of the device and a dual VM-CIM can be attached to the hub.

Help for Choosing USB Profiles

When you are connected to a KVM target server in VKC, you can view information about USB profiles via the Help on USB Profiles command on the USB Profile menu.



USB profile help appears in the USB Profile Help window. For detailed information about specific USB profiles, see ***Available USB Profiles*** (on page 186) and the release notes that came with each firmware upgrade.

Raritan provides a standard selection of USB configuration profiles for a wide range of operating system and BIOS level server implementations. These are intended to provide an optimal match between remote USB device and target server configurations.

The 'Generic' profile meets the needs of most commonly deployed target server configurations.

Additional profiles are made available to meet the specific needs of other commonly deployed server configurations (e.g. Linux, MAC OS-X).

There are also a number of profiles (designated by platform name and BIOS revision) that have been tailored to enhance Virtual Media function compatibility with the target server, for example, when operating at the BIOS level.

'Add Other Profiles' provides access to other profiles available on the system. Profiles selected from this list will be added to the USB Profile Menu. This includes a set of 'trouble-shooting' profiles intended to help identify configuration limitations.

The USB Profile Menu selections are configurable via the Console Device Settings > Port Configuration page.

Should none of the standard USB profiles provided by Raritan meet your target server requirements, Raritan Technical Support can work with you to arrive at a solution tailored for that target. Raritan recommends that you do the following:

1. Check the most recent release notes on the Raritan website (www.raritan.com) on the Firmware Upgrade page to see if a solution is already available for your configuration.
2. If not, please provide the following information when contacting Raritan Technical Support:
    a. Target server information, manufacturer, model, BIOS
    b. The intended use (e.g. redirecting an image to reload a server's operating system from CD)

CIMs

Windows 3-Button Mouse on Linux Targets

When using a 3-button mouse on a Windows client connecting to a Linux target, the left mouse button may get mapped to the center button of the Windows client 3-button mouse.

KX-to-KX II Access via a VM-CIM

If you are using the local port of a Dominion KX II target and accessing it via another KX, use a DCIM.

Virtual Media

Virtual Media Not Refreshed After Files Added

After a virtual media drive has been mounted, if you add a file(s) to that drive, those files may not be immediately visible on the target server. Disconnect and then reconnect the virtual media connection.

Target BIOS Boot Time with Virtual Media

The BIOS for certain targets may take longer to boot if media is mounted virtually at the target.

➢ ***To shorten the boot time:***

1. Close the Virtual KVM Client to completely release the virtual media drives.
2. Restart the target.

CC-SG

Virtual KVM Client Version Not Known from CC-SG Proxy Mode

When the Virtual KVM Client is launched from CommandCenter Secure Gateway (CC-SG) in proxy mode, the Virtual KVM Client version is unknown. In the About Raritan Virtual KVM Client dialog, the version is displayed as “Version Unknown”.

Proxy Mode and MPC

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

Appendix D FAQs

In This Chapter

General Questions

What is the Dominion KX II?

The Dominion KX II is a second generation KVM-over-IP switch that enables IT administrators to access and control servers over a network with BIOS-level functionality. The Dominion KX II is completely hardware and OS-independent. Users can troubleshoot and reconfigure servers even when servers are down.

At the rack, the Dominion KX II provides the same functionality, convenience, space savings, and cost savings as traditional KVM switches. However, the Dominion KX II also integrates the industry's highest-performing KVM-over-IP technology, allowing multiple administrators to access server KVM consoles from any networked workstation.

How does Dominion KX II differ from remote control software?

When using the Dominion KX II remotely, at first glance, the interface may seem similar to remote control software such as pcAnywhere, Windows Terminal Services/Remote Desktop, VNC, and so forth. However, because the Dominion KX II is not a software but a hardware solution, it's much more powerful. Specifically:

- State-Independent/Agentless - The Dominion KX II does not require the managed server OS to be up and running, nor does it require any special software to be installed on the managed server.
- Out-of-Band - Even if the managed server's own network connection is unavailable, it can still be managed through the Dominion KX II.
- BIOS-Level Access - Even if the server is hung at boot up, requires booting to safe mode, or requires system BIOS parameters to be altered, the Dominion KX II still works flawlessly to enable these configurations to be made.

How do the new features of the Dominion KX II compare to the KX I?

The Dominion KX II has many new and exciting features, including virtual media, absolute mouse synchronization, dual power, dual gigabit Ethernet, common web-based user interfaces, next generation local port, and more.

How do I migrate from the Dominion KX I to Dominion KX II?

In general, customers can continue to use their existing switches for many years. As their data centers expand, customers can purchase and use the new Dominion KX II models. Raritan's centralized management unit, CommandCenter Secure Gateway, and the Multi-Platform Client (MPC) both support KX I and Dominion KX II switches seamlessly.

Will my existing KX I CIMs work with the Dominion KX II switch?

Yes, existing KX I CIMs will work with the Dominion KX II switch. In addition, select Paragon CIMs will work with the Dominion KX II. This provides an easy migration to the Dominion KX II from Paragon I customers who wish to switch to KVM-over-IP.

Can the Dominion KX II be rack mounted?

Yes. The Dominion KX II ships standard with 19" rack mount brackets. It can also be reverse rack mounted so the server ports face forward.

How large is the Dominion KX II?

The Dominion KX II is only 1U high (except KX2-464, which is 2U), fits in a standard 19" rack mount, and is only 11.4" (29 cm) deep.

Remote Access

How many users can remotely access servers on each Dominion KX II?

The Dominion KX II models offer remote connections for up to eight users per channel for simultaneous access and control of a unique target server. For one-channel devices like the DKX2-116, up to eight remote users can access and control a single target server. For two-channel devices, like the DKX2-216, up to eight users can access and control the server on channel one and up to another eight users on channel two. For four-channel devices, up to eight users per channel, for a total of 32 (8 x 4) users, can access and control four servers in a similar fashion.

Can two people look at the same server at the same time?

Yes, actually up to eight people can access and control any single server at the same time.

Can two people access the same server, one remotely and one from the local port?

Yes, the local port is completely independent of the remote “ports.” The local port can access the same server using the PC-Share feature.

In order to access Dominion KX II from a client, what hardware, software or network configuration is required?

Because the Dominion KX II is completely web-accessible, it doesn't require installation of proprietary software on clients used for access.

The Dominion KX II can be accessed through major web browsers including Internet Explorer, Mozilla, and Firefox. The Dominion KX II can now be accessed on Windows, Linux, Sun Solaris and Macintosh desktops, via Raritan's Java-based Multi-Platform Client (MPC) and the new Virtual KVM Client.

The Dominion KX II administrators can also perform remote management (set passwords and security, rename servers, change IP address, and so forth.) using a convenient browser-based interface.

What is the file size of the Virtual KVM Client applet that is used to access Dominion KX II? How long does it take to retrieve?

The Virtual KVM Client applet used to access the Dominion KX II is approximately 500KB in size. The following chart describes the approximate time required to retrieve the Dominion KX II's applet at different network speeds:

Speed	Description	Time
100Mbps	Theoretical 100Mbit network speed	0.05 seconds
60Mbps	Likely practical 100Mbit network speed	0.08 seconds
10Mbps	Theoretical 10Mbit network speed	.4 seconds
6Mbps	Likely practical 10Mbit network speed	.8 seconds
512Kbps	Cable modem download speed (typical)	8 seconds

How do I access servers connected to Dominion KX II if the network ever becomes unavailable?

The Dominion KX II's local ports always allow access to servers from the rack, regardless of the network condition.

Do you have a non-Windows client?

Yes. Both the Virtual KVM Client and the Multi-Platform Client (MPC), allow non-Windows users to connect to KVM target servers through the Dominion KX I and Dominion KX II switches. MPC can be run via web browsers and standalone. Refer to ***Virtual KVM Client*** (on page 50) and ***Raritan Multi-Platform Client (MPC) Supported Operating Systems*** (on page 87) for more information.

Sometimes during a Virtual KVM Client session, the Alt key appears to get stuck. What should I do?

This usually occurs in situations when the Alt key is held and not released. For instance, continuing to press the Alt key while pressing the space bar might cause the focus to change from the target server to the client PC.

The local operating system then interprets this key combination and consequently triggers the action for this key combination in the active window (the client PC).

Universal Virtual Media

What Dominion KX II models support virtual media?

All of the Dominion KX II models support virtual media. It is available standalone and through Raritan's CommandCenter Secure Gateway, a centralized management unit.

What types of virtual media does the Dominion KX II support?

The Dominion KX II supports the following types of media: internal and USB-connected CD/DVD drives, USB mass storage devices, PC hard drives, and ISO images.

Is virtual media secure?

Yes. Virtual media sessions are secured using 128-bit AES or RC4 encryption.

What is required for virtual media?

A Dominion KX II virtual media CIM is required. There are two of these CIMs: the D2CIM-VUSB and the new D2CIM-DVUSB.

The D2CIM-DVUSB has dual USB connectors and provides high speed operation for virtual media and independent low speed operation for keyboard and mouse. It is recommended for customers wishing to access virtual media at the BIOS level. The D2CIM-VUSB has a single USB connector and is for customers who would like to access virtual media at the OS, but not the BIOS level.

USB Profiles

What is a USB profile?

Certain servers require a specifically configured USB interface for USB based services such as virtual media. The USB Profile tailors the Dominion KX II's USB interface to the server to accommodate these server specific characteristics.

Why do I need to use a USB profile?

USB profiles enable the Dominion KX II to connect to a wide variety of KVM target servers using a USB connection. While the Generic USB profile will work with the vast majority of target servers, other profiles are provided for use with particular BIOS and operating system configurations such as Mac OS X and Linux.

How is a USB profile used?

Individual or groups of ports can be configured by the administrator to use a specific USB profile in the Dominion KX II's Port Configuration pages.

A USB profile can also be selected in the Dominion KX II client when required.

What happens if I don't choose the correct USB profile?

Not choosing the right USB profile for a KVM target server can prevent a mass storage device, mouse, or keyboard from working optimally or working at all.

Do I always need to set a USB profile when I use virtual media?

No, in many cases, the default USB Profile is sufficient when using virtual media at the OS level or operating at the BIOS level without accessing virtual media.

What profiles are available?

See ***Available USB Profiles*** (on page 186).

How do I know which USB profile is best for a given target server?

The Generic profile is best for the vast majority of target servers. If this profile does not work with a given KVM target server, you can choose the appropriate USB profile in ***Available USB Profiles*** (on page 186). Select the profile that best matches your target server.

What is the purpose of a BIOS profile?

A BIOS profile has been tailored to match the requirements of a particular server's BIOS that does not implement the full USB specification. The profile enables use of keyboard, mouse, and virtual media at the BIOS level, overcoming the restrictions or limitations of the BIOS.

Do I need a special CIM to use USB profiles?

You must use a D2CIM-VUSB or D2CIM-DVUSB with updated firmware.

Will Raritan provide USB profiles for other target server configurations?

Raritan will provide new USB profiles to suit customer needs. As these profiles become available, they will be included in firmware upgrades.

Ethernet and IP Networking

Does the Dominion KX II offer dual gigabit Ethernet ports to provide redundant fail-over?

Yes. The Dominion KX II features dual gigabit Ethernet ports to provide redundant failover capabilities. Should the primary Ethernet port (or the switch/router to which it is connected) fail, the Dominion KX II will failover to the secondary network port with the same IP address, ensuring that server operations are not disrupted. Note that automatic failover must be enabled by the administrator.

How is bandwidth used in KVM-over-IP systems?

The Dominion KX II offers next generation KVM-over-IP technology – the very best video compression available. Raritan has received numerous technical awards confirming its high video quality transmissions and the low bandwidth utilization.

The Dominion KX II digitizes, compresses and encrypts the keyboard, video, and mouse signals from the target server and transmits IP packets over the IP network to the remote client to create the remote session to the user. The Dominion KX II provides an at-the-rack experience based on its industry leading video processing algorithms.

Screen changes, such as video, accounts for the majority of the bandwidth used – keyboard and mouse activity is significantly less.

It is important to note that bandwidth is only used when the user is active. The amount of bandwidth used is based on the amount of change to the server's video display screen.

If there are no changes to the video – the user is not interacting with the server – there is generally no bandwidth used. If the user moves the mouse or types a character, then there is a small amount of bandwidth used. If the display is running a complex screen saver or playing a video, then there can be a larger amount of bandwidth used.

How does bandwidth affect KVM-over-IP performance?

In general, there is a trade-off between bandwidth and performance. The more bandwidth available, the better performance can be. In limited bandwidth environments, performance can degrade. The Dominion KX II has been optimized to provide strong performance in a wide variety of environments.

What factors affect bandwidth?

There are many factors that determine how much bandwidth will be used. The primary factor, as discussed previously, is the amount of change in the target server's video display. This is dependent on the user's task and actions.

Other factors include the server's video resolution, networking speed and characteristics, client PC resources, and video card noise.

The Dominion KX II has very sophisticated video processing algorithms that optimize bandwidth and performance for a variety of environments. In addition, they are highly configurable since there are many settings to optimize bandwidth usage. In particular, the Connection Speed setting in the remote clients (VKC, MPC) can be set to reduce the bandwidth used.

Unlike KX I, the Noise Filter parameter does not generally have a large role in reducing bandwidth or improving performance.

How much bandwidth does Dominion KX II use for common tasks?

Bandwidth primarily depends on the user's task and actions. The more the server's video screen changes, the more bandwidth is utilized.

The table below summarizes some standard use cases using the Dominion KX II's default and with two reduced bandwidth settings (Connection Speed setting of 1Mb with 15 and 8 bit color) on a Windows XP target server (1024x768 resolution) over a 100 Mbit/s LAN:

User task	Default	1Mb speed & 15 bit color	1Mb speed & 8 bit color
Idle Windows Desktop	0 KB/s	0 KB/s	0 KB/s
Move mouse cursor	5 - 15 KB/s	2 - 6 KB/s	2 - 3 KB/s
Drag icon	40 - 70 KB/s	10-25 KB/s	5 - 15 KB/s
Drag folder	10 - 40 KB/s	5 - 20 KB/s	5 - 10 KB/s
Open text window	50 - 100 KB/s	25 - 50 KB/s	10 - 15 KB/s
Continuous typing	1 KB/s	.5 - 1 KB/s	.2 - .5 KB/s
Scroll text window	10 - 50 KB/s	5 -25 KB/s	2 - 10 KB/s
Close text window	50 - 100 KB/s	20 - 40 KB/s	10 - 15 KB/s
Open panel	50 - 100 KB/s	60 - 70 KB/s	20 - 30 KB/s

User task	Default	1Mb speed & 15 bit color	1Mb speed & 8 bit color
Change tab in panel	40 - 50 KB/s	20 - 50 KB/s	10 - 20 KB/s
Close panel	50 - 100 KB/s	40 - 60 KB/s	20 - 30 KB/s
Change panel option	2 - 10 KB/s	1 - 5 KB/s	1- 3 KB/s
Open browser page	100 - 300 KB/s	50 - 200 KB/s	40 - 80 KB/s
Scroll browser	75 - 200 KB/s	50 - 200 KB/s	30 - 100 KB/s
Close browser	100 - 150 KB/s	75 - 100 KB/s	30 - 60KB/s
Open Start menu	75 - 100 KB/s	50 -75 KB/s	20 - 30 KB/s
Close Start menu	75 - 100 KB/s	25 - 50 KB/s	10 - 15 KB/s
Starfield screen saver	25 - 50 KB/s	10 - 15 KB/s	7 - 10 KB/s
3D pipes screen saver	10 - 100 KB/s	5 - 20 KB/s	2 - 10 KB/s
Windows media video	500 - 1200 KB/s	300 - 500 KB/s	150 - 300 KB/s
QuickTime video #1	700 - 2500 KB/s	400 - 500 KB/s	150 - 350 KB/s
QuickTime video #2	1500 - 2500 KB/s	400 - 550 KB/s	200 - 350 KB/s

With the reduced bandwidth settings, bandwidth is reduced significantly for virtually all tasks. With the 15 bit color setting, perceived performance is similar to the default parameters. Further, bandwidth reductions are possible with additional changes in the settings.

Please note that these bandwidth figures are only examples and may vary from those seen in your environment due to many factors.

How can I reduce bandwidth?

The Dominion KX II provides a variety of settings in our remote clients to optimize bandwidth and performance. The default settings will provide an at-the-rack level of performance in standard LAN/WAN environments with economical use of bandwidth.

Bandwidth management settings include the Connection Speed and Color Depth. To reduce bandwidth:

Reduce Connection Speed

Reducing the connection speed can significantly reduce the bandwidth used. In standard LAN/WAN environments, setting the connection speed to 1.5 or 1Mbit per second will reduce bandwidth while maintaining good performance. Settings below this will further reduce bandwidth and are appropriate for slow bandwidth links.

Reduce Color Depth

Reducing the color depth will also significantly decrease bandwidth and increase performance, but fewer colors will be used, resulting in video degradation. This may be acceptable for certain system administration tasks.

For slow Internet connections, use of 8 bit color or lower bit depths can reduce bandwidth and improve performance.

Other tips to decrease bandwidth include:

- Use a solid desktop background instead of a complex image
- Disable screen savers
- Use a lower resolution on the target server
- Uncheck the “Show window contents while dragging” option in Windows
- Use simple images, themes and desktops (for example. Windows Classic).

What should I do on slower bandwidth links?

The connection speed and color depth settings can be tweaked to optimize performance for slower bandwidth links. For example, in the Multi-Platform Client or the Virtual KVM Client, set the connection speed to 1.5Mb or 1Mb and the color depth to 8 bit. Even lower connection speeds and color depths can be used for very low bandwidth situations.

I want to connect over the Internet. What type of performance should I expect?

It depends on the bandwidth and latency of the Internet connection between your remote client and the Dominion KX II. With a cable modem or high speed DSL connection, your performance can be very similar to a LAN/WAN connection. For lower speed links, use the suggestions above to improve performance.

I have a high bandwidth environment. How can I optimize performance?

The default settings will provide strong performance in a high bandwidth environment. Ensure that the connection speed is set to 100Mb or 1Gb and the color depth is set to15 bit RGB Color.

What is the speed of the Dominion KX II's Ethernet interfaces?

The Dominion KX II supports gigabit as well as 10/100 Ethernet. The Dominion KX II supports two 10/100/1000 speed Ethernet interfaces, with configurable speed and duplex settings (either autodetected or manually set).

Can I access the Dominion KX II over a wireless connection?

Yes. The Dominion KX II not only uses standard Ethernet, but also very conservative bandwidth with very high quality video. Thus, if a wireless client has network connectivity to the Dominion KX II, servers can be configured and managed at BIOS-level wirelessly.

Can the Dominion KX II be used over the WAN (Internet), or just over the corporate LAN?

Whether via a fast corporate LAN, the less predictable WAN (Internet), cable modem or dial-up modem, the Dominion KX II's KVM-over-IP technology can accommodate the connection.

Can I use the Dominion KX II with a VPN?

Yes, the Dominion KX II uses standard Internet Protocol (IP) technologies from Layer 1 through Layer 4. Traffic can be easily tunneled through standard VPNs.

How many TCP ports must be open on my firewall in order to enable network access to the Dominion KX II? Are these ports configurable?

Only one. The Dominion KX II protects network security by only requiring access to a single TCP port to operate. This port is completely configurable for additional security.

Note that, of course, to use the Dominion KX II's optional web browser capability, the standard HTTPS port 443 must also be open.

Does the Dominion KX II require an external authentication server to operate?

No. The Dominion KX II is a completely self-sufficient. After assigning an IP address to the Dominion KX II, it is ready to use. It's web browser and authentication capabilities are completely built-in.

If an external authentication server (such as LDAP, Active Directory, RADIUS, etc.) is used, the Dominion KX II allows this as well, and will even failover to its own internal authentication should the external authentication server become unavailable. In this way, the Dominion KX II's design philosophy is optimized to provide ease of installation, complete independence from any external server, and maximum flexibility.

Can the Dominion KX II be used with CITRIX?

Dominion KX II may work with remote access products like CITRIX if configured appropriately, but Raritan cannot guarantee it will work with acceptable performance. Products like CITRIX utilize video redirection technologies similar in concept to digital KVM switches so that two KVM-over-IP technologies are being used simultaneously.

Can the Dominion KX II use DHCP?

DHCP addressing can be used, however, Raritan recommends fixed addressing since the Dominion KX II is an infrastructure device and can be accessed and administered more effectively with a fixed IP address.

I'm having problems connecting to the Dominion KX II over my IP network. What could be the problem?

The Dominion KX II relies on your LAN/WAN network. Some possible problems include:

- Ethernet autonegotiation - On some networks, 10/100 autonegotiation does not work properly and the Dominion KX II unit must be set to 100MB/full duplex or the appropriate choice for its network.
- Duplicate IP address - If the IP address of the Dominion KX II is the same as another device, network connectivity may be inconsistent.
- Port 5000 conflicts - If another device is using port 5000, the Dominion KX II default port must be changed (or the other device must be changed).

When changing the IP address of the Dominion KX II or swapping in a new Dominion KX II, sufficient time must be allowed for its IP and MAC addresses to be known throughout the Layer 2 and Layer 3 networks.

Servers

Does the Dominion KX II depend on a Windows server to operate?

Absolutely not. Because users depend on the KVM infrastructure to always be available in any scenario whatsoever (as they will likely need to use the KVM infrastructure to fix problems), the Dominion KX II is designed to be completely independent from any external server. For example, should the data center come under attack from a malicious Windows worm or virus, administrators will need to use the KVM solution to resolve the situation. Therefore, it is imperative that the KVM solution, in turn, must not rely on these same Windows servers (or any server, for that matter) to be operational in order for the KVM solution to function.

To this end, the Dominion KX II is completely independent. Even if a user chooses to configure the Dominion KX II to authenticate against an Active Directory server - if that Active Directory server becomes unavailable, the Dominion KX II's own authentication will be activated and fully functional.

Do I need to install a web server such as Microsoft Internet Information Services (IIS) in order to use the Dominion KX II's web browser capability?

No. The Dominion KX II is a completely self-sufficient device. After assigning an IP address to the Dominion KX II, it's ready to use since it comes with web browser and authentication capabilities completely built-in.

What software do I have to install in order to access the Dominion KX II from a particular workstation?

None. The Dominion KX II can be accessed completely via a web browser (although an optional installed client is provided on Raritan's website for the purpose of accessing the Dominion KX II via modem). A Java-based client is now available for non-Windows users.

What should I do to prepare a server for connection to the Dominion KX II?

Simply set the mouse parameters in order to provide users with the best mouse synchronization during remote connections, as well as turning off the power management features that effect screen display. However, if the new D2CIM-VUSB adapter is used (supporting Absolute Mouse Synchronization™), then manually setting the mouse parameters isn't necessary.

Installation

Besides the unit itself, what do I need to order from Raritan to install the Dominion KX II?

Each server that connects to the Dominion KX II requires a Dominion or Paragon Computer Interface Module (CIM), an adapter that connects directly to the keyboard, video, and mouse ports of the server.

What kind of Cat5 cabling should be used in my installation?

The Dominion KX II can use any standard UTP (unshielded twisted pair) cabling, whether Cat5, Cat5e, or Cat6. Often in our manuals and marketing literature, Raritan will simply say “Cat5” cabling for short. In actuality, any brand UTP cable will suffice for the Dominion KX II.

What types of servers can be connected to the Dominion KX II?

The Dominion KX II is completely vendor independent. Any server with standard-compliant keyboard, video, and mouse ports can be connected.

How do I connect servers to the Dominion KX II?

Servers that connect to the Dominion KX II require a Dominion or Paragon CIM, which connects directly to the keyboard, video, and mouse ports of the server. Then, connect each CIM to Dominion KX II using standard UTP (twisted pair) cable such as Cat5, Cat5e, or Cat6.

How far can my servers be from the Dominion KX II?

In general servers can be up to 150 feet (45 m) away from the Dominion KX II depending on the type of server. Refer to the Raritan website (www.raritan.com) or ***Target Server Connection Distance and Video Resolution*** (on page 299) for more information.) For the new D2CIM-VUSB CIM that supports virtual media and Absolute Mouse Synchronization, a 100 (30 m) foot range is recommended.

Some operating systems lock up when I disconnect a keyboard or mouse during operation. What prevents servers connected to the Dominion KX II from locking up when I switch away from them?

Each Dominion computer interface module (DCIM) dongle acts as a virtual keyboard and mouse to the server to which it is connected. This technology is called KME (keyboard/mouse emulation). Raritan's KME technology is data center grade, battle-tested, and far more reliable than that found in lower-end KVM switches: it incorporates more than 15 years of experience and has been deployed to millions of servers worldwide.

Are there any agents that must be installed on servers connected to the Dominion KX II?

Servers connected to the Dominion KX II do not require any software agents to be installed, because Dominion KX II connects directly via hardware to servers' keyboard, video, and mouse ports.

How many servers can be connected to each the Dominion KX II unit?

The Dominion KX II models range from 8, 16, or 32 server ports in a 1U chassis to 64 server ports in a 2U chassis. This is the industry's highest digital KVM switch port density.

What happens if I disconnect a server from Dominion KX II and reconnect it to another Dominion KX II unit, or connect it to a different port on the same Dominion KX II unit?

Dominion KX II will automatically update the server port names when servers are moved from port to port. Furthermore, this automatic update does not just affect the local access port, but propagates to all remote clients and the optional CommandCenter Secure Gateway management appliance.

How do I connect a serially controlled (RS-232) device to Dominion KX II, such as a Cisco router/switch or a headless Sun server?

If there are only a few serially-controlled devices, they may be connected to a Dominion KX II using Raritan's new P2CIM-SER serial converter.

However, if there are four or more serially-controlled devices, we recommend the use of Raritan's KSX II line or SX line of secure console servers. These devices are easy to use, configure and manage, and can be completely integrated with a Dominion Series deployment. In particular, many UNIX and networking administrators appreciate the ability to directly SSH to a device.

Local Port

Can I access my servers directly from the rack?

Yes. At the rack, the Dominion KX II functions just like a traditional KVM switch, allowing control of up to 64 servers using a single keyboard, monitor, and mouse.

When I am using the local port, do I prevent other users from accessing servers remotely?

No. The Dominion KX II local port has a completely independent access path to the servers. This means a user can access servers locally at the rack without compromising the number of users that access the rack remotely at the same time.

Can I use a USB keyboard or mouse at the local port?

Yes. The Dominion KX II offers both PS/2 and USB keyboard and mouse ports on the local port. Note that the USB ports are USB v1.1, and support keyboards and mice only, not USB devices such as scanners or printers.

Is there an Onscreen Display for local, at-the-rack access?

Yes, but the Dominion KX II's at-the-rack access goes way beyond conventional OSDs. Featuring the industry's first browser-based interface for at-the-rack access, the Dominion KX II's local port uses the same interface for local and remote access. Moreover, most administrative functions are available at-the-rack.

How do I select between servers while using the local port?

The local port displays the connected servers using the same user interface as the remote client. Connect to a server with a simple click of the mouse.

How do I ensure that only authorized users can access servers from the local port?

Users attempting to use the local port must pass the same level of authentication as those accessing remotely. This means that:

- If the Dominion KX II is configured to interact with an external RADIUS, LDAP, or Active Directory server, users attempting to access the local port will authenticate against the same server.
- If the external authentication servers are unavailable, the Dominion KX II fails-over to its own internal authentication database.

- The Dominion KX II has its own standalone authentication, enabling instant, out-of-the-box installation.

If I use the local port to change the name of a connected server, does this change propagate to remote access clients as well? Does it propagate to the optional CommandCenter unit?

Yes. The local port presentation is identical and completely in sync with remote access clients, as well as Raritan's optional CommandCenter Secure Gateway management device. To be clear, if the name of a server via the Dominion KX II onscreen display is changed, this updates all remote clients and external management servers in real-time.

If I use the Dominion KX II's remote administration tools to change the name of a connected server, does that change propagate to the local port OSD as well?

Yes. If the name of a server is changed remotely, or via Raritan's optional CommandCenter Secure Gateway management unit, this update immediately affects the Dominion KX II's onscreen display.

Sometimes I see "shadows" on the local port user interface. Why does that occur?

This shadow/ghosting effect may occur with LCD monitors that have been on for long periods. The LCD properties and the electrical/static charge can produce these effects when the screen is on for a long time.

Power Control

Does Dominion KX II have a dual power option?

All of the Dominion KX II models come equipped with dual AC inputs and power supplies with automatic fail-over. Should one of the power inputs or power supplies fail, then the Dominion KX II will automatically switch to the other.

Does the power supply used by the Dominion KX II automatically detect voltage settings?

Yes. The Dominion KX II's power supply can be used in AC voltage ranges from 100-240 volts, at 50-60 Hz.

If a power supply or input fails, will I be notified?

The Dominion KX II front panel LED will notify the user of a power failure. An entry will also be sent to the Audit Log and displayed on the Dominion KX II Remote Client User Interface. If configured by the administrator, then SNMP or Syslog events will be generated.

What type of power control capabilities does the Dominion KX II offer?

Raritan's Remote Power Control power strips can be connected to the Dominion KX II to provide power control of the KVM target servers. After a simple one-time configuration step, just right click the server name to power on, off, or recycle a hung server. Note that a hard reboot provides the physical equivalent of unplugging the server from the AC power line, and reinserting the plug.

Does the Dominion KX II support servers with multiple power supplies? What if each power supply is connected to a different power strip?

Yes. The Dominion KX II can be easily configured to support multiple power supplies connected to multiple power strips. Up to eight (8) power strips can be connected to the Dominion KX II device. Four power supplies can be connected per target server to multiple power strips.

Does remote power control require any special server configuration?

Some servers ship with default BIOS settings such that the server does not automatically restart after losing and regaining power. See the server user guide for more information.

What type of power strips does the Dominion KX II support?

To take advantage of the Dominion KX II's integrated power control user interface, and more importantly, integrated security, use Raritan's Remote Power Control (RPC) power strips. RPCs come in many outlet, connector, and amp variations. The D2CIM-PWR must be purchased to connect the RPC to the Dominion KX II.

Scalability

How do I connect multiple Dominion KX II devices together into one solution?

Multiple Dominion KX II devices do not need to be physically connected together. Instead, each Dominion KX II device connects to the network. They automatically work together as a single solution if deployed with Raritan's optional CommandCenter Secure Gateway (CC-SG) management unit. CC-SG acts as a single access point for remote access and management. CC-SG offers a significant set of convenient tools, such as consolidated configuration, consolidated firmware update, and a single authentication and authorization database.

In addition, CC-SG enables sophisticated server sorting, permissions, and access. If deployment of Raritan's CC-SG management unit isn't an option, multiple Dominion KX II devices still interoperate and scale automatically. The Dominion KX II's remote user interface and the Multi-Platform Client will automatically discover Dominion KX II devices. Non-discovered Dominion KX II devices can be accessed via a user-created profile.

Can I connect an existing analog KVM switch to the Dominion KX II?

Yes. Analog KVM switches can be connected to one of the Dominion KX II's server ports. Simply use a PS/2 Computer Interface Module (CIM) and attach it to the user ports of the existing analog KVM switch. Please Note that analog KVM switches vary in their specifications and Raritan cannot guarantee the interoperability of any particular third-party analog KVM switch. Contact Raritan technical support for further information.

Computer Interface Modules (CIMs)

Can I use Computer Interface Modules (CIMs) from Raritan's analog matrix KVM switch, Paragon, with the Dominion KX II?

Yes. Certain Paragon computer interface modules (CIMs) may work with the Dominion KX II (check the Raritan Dominion KX II release notes on the website for the latest list of certified CIMs).

However, because Paragon CIMs cost more than Dominion KX II CIMs (as they incorporate technology for video transmission of up to 1000 feet [300 meters]), it is not generally advisable to purchase Paragon CIMs for use with the Dominion KX II. Also note that when connected to the Dominion KX II, Paragon CIMs transmit video at a distance of up to 150 feet, the same as the Dominion KX II CIMs; not at 1000 feet [300 meters], as they do when connected to Paragon.

Can I use the Dominion KX II Computer Interface Modules (CIMs) with Raritan's analog matrix KVM switch, Paragon?

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

Security

What kind of encryption does the Dominion KX II use?

The Dominion KX II uses industry-standard (and extremely secure) 128-bit RC4 or AES encryption, both in its SSL communications as well as its own data stream. Literally no data is transmitted between remote clients and the Dominion KX II that is not completely secured by encryption.

Does the Dominion KX II support AES encryption as recommended by the US Government's NIST and FIPs standards?

The Dominion KX II utilizes the Advanced Encryption Standard (AES) encryption for added security.

AES is a US government approved cryptographic algorithm that is recommended by the National Institute of Standards and Technology (NIST) in the FIPS Standard 197.

Does the Dominion KX II allow encryption of video data? Or does it only encrypt keyboard and mouse data?

Unlike competing solutions, which only encrypt keyboard and mouse data, the Dominion KX II does not compromise security; it allows encryption of keyboard, mouse and video data.

How does the Dominion KX II integrate with external authentication servers such as Active Directory, RADIUS, or LDAP?

Through a very simple configuration, the Dominion KX II can be set to forward all authentication requests to an external server such as LDAP, Active Directory, or RADIUS. For each authenticated user, the Dominion KX II receives the user group to which that user belongs from the authentication server. The Dominion KX II then determines the user's access permissions depending on the user group to which he or she belongs.

How are usernames and passwords stored?

Should the Dominion KX II's internal authentication capabilities be used, all sensitive information such as usernames and passwords are stored in an encrypted format. Literally no one, including Raritan Technical Support or Product Engineering departments, can retrieve those usernames and passwords.

Does the Dominion KX II support strong password?

Yes, the Dominion KX II has administrator-configurable, strong password checking to ensure that user-created passwords meet corporate and/or government standards and are resistant to brute force hacking.

If the Dominion KX II encryption mode is set to Auto, what level of encryption is achieved?

The encryption level that is autonegotiated is dependent on the browser in use:

Browser	Encryption Level
Internet Explorer 6	RC4
Internet Explorer 7	AES-128
Firefox 1.5	RC4
Firefox 2.0	RC4
Mozilla 1.7	RC4
Safari 2.0.4	AES-128

Manageability

Can the Dominion KX II be remotely managed and configured via web browser?

Yes, the Dominion KX II can be completely configured remotely via web browser. Note that this does require that the workstation have an appropriate Java Runtime Environment (JRE) version installed.

Besides the initial setting of the Dominion KX II's IP address, everything about the solution can be completely set up over the network. (In fact, using a crossover Ethernet cable and the Dominion KX II's default IP address, you can even configure the initial settings via web browser.)

Can I backup and restore the Dominion KX II's configuration?

Yes, the Dominion KX II's device and user configurations can be completely backed up for later restoration in the event of a catastrophe.

The Dominion KX II's backup and restore functionality can be used remotely over the network or via the Remote Console.

What auditing or logging does Dominion KX II offer?

For complete accountability, the Dominion KX II logs all major user and system events with a date and time stamp. For instance, reported events include (but are not limited to): user login, user log off, user access of a particular server, unsuccessful login, configuration changes, and so forth.

Can the Dominion KX II integrate with Syslog?

Yes. In addition to the Dominion KX II's own internal logging capabilities, the Dominion KX II can send all logged events to a centralized Syslog server.

Can the Dominion KX II integrate with SNMP?

Yes. In addition to the Dominion KX II's own internal logging capabilities, the Dominion KX II can send SNMP traps to SNMP management systems like HP Openview and Raritan's CC-NOC.

Can the Dominion KX II's internal clock be synchronized with a timeserver?

Yes, the Dominion KX II supports the industry-standard NTP protocol for synchronization with either a corporate timeserver or with any public timeserver (assuming that outbound NTP requests are allowed through the corporate firewall).

Miscellaneous

What is the Dominion KX II's default IP address?

192.168.0.192

What is the Dominion KX II's default user name and password?

The Dominion KX II's default user name is admin and the default password is raritan [all lower case]. However, for the highest level of security, the Dominion KX II forces the administrator to change the Dominion KX II default administrative user name and password when the unit is first booted up.

I changed and subsequently forgot the Dominion KX II's administrative password; can you retrieve it for me?

The Dominion KX II contains a hardware reset button that can be used to factory reset the device, which will reset the administrative password on the device.

I am logged into the Dominion KX II using Firefox, and I opened another Firefox browser. I am automatically logged into the same Dominion KX II with the second Firefox browser. Is this right?

Yes, this is correct behavior and is the direct result of how browsers and cookies function.

I am logged into the Dominion KX II using Firefox and I attempt to log into another Dominion KX II using another Firefox browser session from the same client. I am logged off of both Dominion KX IIs;. Is this correct behavior?

Yes, to access two different Dominion KX II devices either close the first session or use another client PC.

When I'm running a KVM session using Firefox as my browser and certain dialogs are opened in the Virtual KVM Client (for example, Connection Properties, Video Settings), it seems to block the Firefox browser (even other Firefox sessions). What can I do?

This is normal behavior since all Firefox sessions are associated. Once you close the Virtual KVM Client dialog, Firefox will no longer be blocked.

Index

Raritan.
When you're ready to take control®

➢ U.S./Canada/Latin America

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

➢ China

Beijing

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

Shanghai

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

GuangZhou

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

➢ India

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

➢ Japan

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

➢ Europe

Europe

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

United Kingdom

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

Germany

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

➢ Korea

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

➢ Melbourne, Australia

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

➢ Taiwan

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