Dominion KX II

User Guide
Release 2.3.5

DKX2-v2.3.5-0N-E

March 2011

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.

Contents

Chapter 1 Introduction

In This Chapter

KX II Overview

Raritan's Dominion KX II is an enterprise-class, secure, digital KVM (Keyboard, Video, Mouse) switch that provides BIOS-level (and up) access and control of servers from anywhere in the world via a web browser. Up to 64 servers can be controlled with a standard KX II. With the KX II 8-user model, up to 32 servers can be controlled with the KX2-832 and up to 64 servers can be controlled with the KX2-864.

The KX II supports up to 8 video channels, allowing up to eight concurrent users to connect to eight different video targets at any given point in time. At the rack, the 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 KX II provide the same levels of control of your servers via a web browser.

The 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, external modem capabilities, and web management. The KX II 8-user model also provides an extended local port located on the back of the device. These features enable you to deliver higher up-time, better productivity, and bulletproof security - at any time from anywhere.

KX II products can operate as standalone appliances and do not rely on a central management device. For larger data centers and enterprises, numerous KX II devices (along with Dominion SX devices 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.

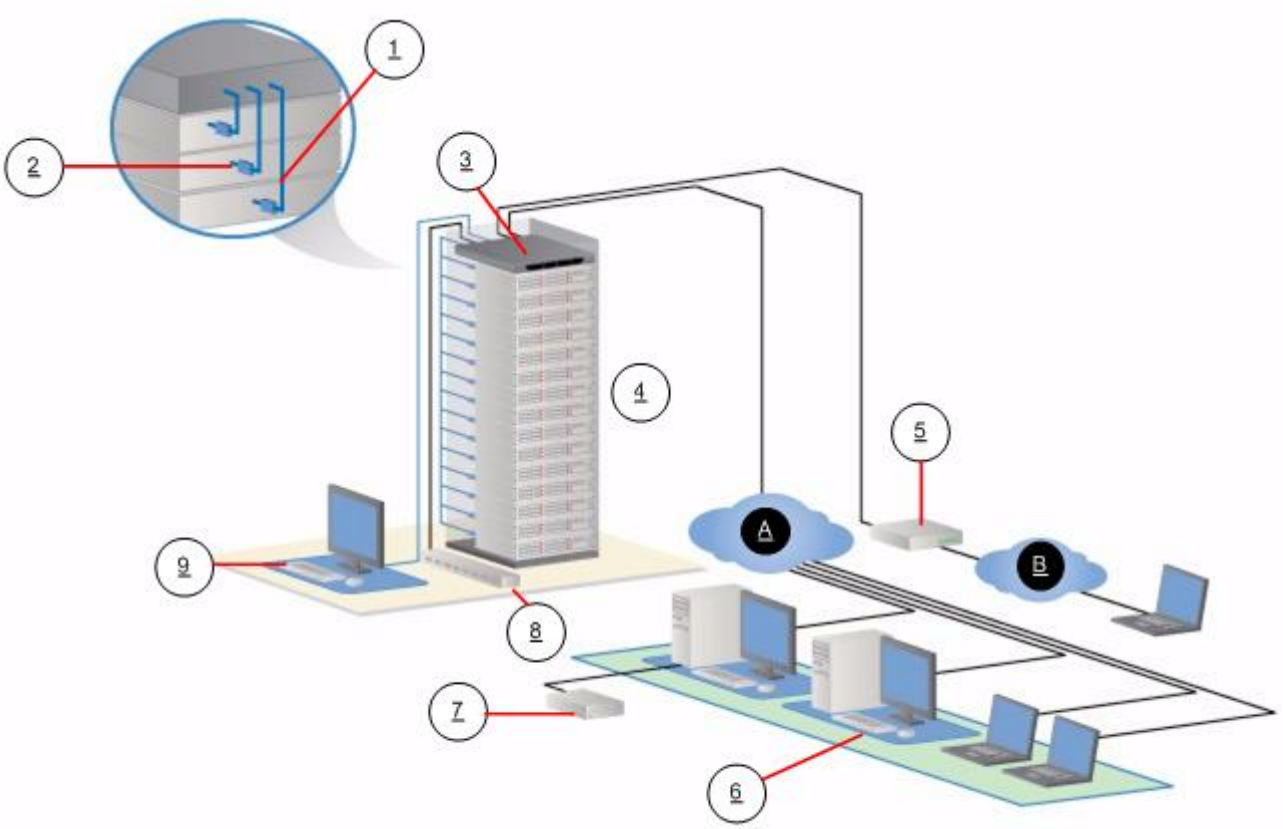


Diagram key			
1	Cat5 cable	7	Remote virtual media USB drive(s)
2	Computer Interface Module (CIM)	8	Rack PDU (power strip)
3	KX II	9	Local access *Note: KX2-832 and KX2-864 also use an extended local port.*
4	Remote KVM and serial devices	A	IP LAN/WAN
5	Modem	B	PSTN
6	Remote (network) access		

KX II Help

The KX II help provides information on how to install, set up, and configure the KX II. It also includes information on accessing target servers and power strips, using virtual media, managing users and security, and maintaining and diagnosing the KX II.

A PDF version of the help can be downloaded from the ***Raritan Firmware and Documentation page http://www.raritan.com/support/firmware-and-documentation/*** on the Raritan website. Raritan recommends that you refer to the Raritan website for the most up-to-date user guides available.

To use online help, Active Content must be enabled in your browser. If you are using Internet Explorer 7, you must enable Scriplets. Consult your browser help for information on enabling these features.

Related Documentation

The KX II help is accompanied by a KX II Device Quick Setup Guide, which can be found on the ***Raritan Firmware and Documentation page http://www.raritan.com/support/firmware-and-documentation/*** of Raritan's website.

Installation requirements and instructions for client applications used with the KX II can be found in the **KVM and Serial Access Clients Guide**, also found on the Raritan website. Where applicable, specific client functions used with the KX II are included in the help.

KX II Client Applications

The following client applications can be used in the KX II:

Product	Works with...				
	MPC	RRC	VKC	RSC	AKC
KX II (Generation 2)	✓		✓		
KX II 2.2 (or later)	✓		✓		✓

See the **KVM and Serial Client Guide** for additional information on the client applications. Also see the ***Working with Target Servers*** (on page 37) section of this guide, which contains information on using the clients with the KX II.

Note: MPC and VKC require the Java™ Runtime Environment (JRE™). AKC is .NET based.

Virtual Media

All 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 KX II models.

Each 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 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. These CIMs also support Absolute Mouse Synchronization™ as well as remote firmware update.

Note: The black connector on the DVUSB CIM is used for keyboard and mouse. The gray connector is used for virtual media. Keep both plugs of the CIM connected to the device. The device may not operate properly if both plugs are not connected to the target server.

Product Photos

KX II

KX2-832

KX2-864

Product Features

Hardware

- Integrated KVM-over-IP remote access
- 1U or 2U 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
- 32 (KX2-832) or 64 (KX2-864) server ports
- Support for tiering in which a base KX II device is used to access multiple other tiered devices. See ***Configuring and Enabling Tiering*** (on page 142) for more information on tiering.
- Up to 8 video channels, depending on the device model, that allows up to 8 users to connect to the KX II at once
- Multiple user capacity (1/2/4/8 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
  - USB 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
- Extended local port on the KX2-832 and KX2-864 models provide extended reach to in-rack access on KX2 devices
- Centralized access security
- Integrated power control
- LED indicators for dual power status, network activity, and remote user status
- Hardware Reset button
- Serial port to connect to an external modem

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
- Smart card/CAC authentication
- SNMP and Syslog management
- IPv4 and IPv6 support
- 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 KX II configuration:

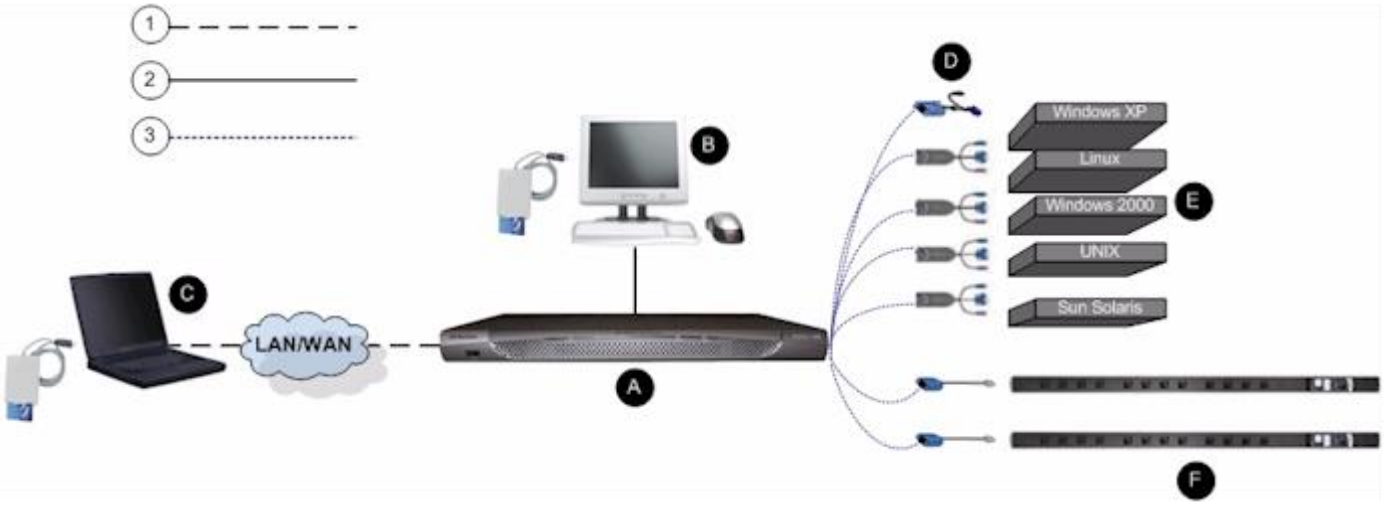


Diagram Key	
1	TCP/IP IPv4 and/or IPv6
2	KVM (Keyboard, Video, Mouse)
3	UTP Cable (Cat5/5e/6)
A	KX II
B	Local Access Console Local User - an optional user console (consisting of a keyboard, mouse, and multi-sync VGA monitor) attached directly to the KX II to control KVM target servers (directly at the rack, not through the network). A USB smart card reader can also be attached at the Local port to mount onto a target server. An extended local port is also provided on the DKX2-832 and DKX2-864 models.
C	Remote PC Networked computers used to access and control KVM target servers connected to the KX II. A USB smart card reader can also be attached to the remote PC and attached to a target server via the KX II.
D	CIMS Dongles that connect to each target server or rack PDU (power strip). Available for all of the supported operating systems.
E	Target Servers KVM Target Servers - servers with video cards and user interfaces (for example, Windows® operating system®, Linux®, Solaris™, etc.) accessed remotely via the KX II.
F	Dominion PX Rack PDU (Power Strips) Raritan rack PDUs accessed remotely via the KX II.

See **Supported CIMs and Operating Systems (Target Servers)** for a list of the supported operating systems and CIMs, and see ***Supported Operating Systems (Clients)*** (on page 260) for a list of the operating systems supported by the KX II remotely.

Package Contents

Each KX II ships as a fully-configured stand-alone product in a standard 1U (2U for DKX2-864) 19" rackmount chassis. Each KX II device ships with the following contents:

Amount included	Item
1	KX II device
1	KX II Quick Setup Guide
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

Chapter 2 Installation and Configuration

In This Chapter

Overview

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 the KX II:

- ***Step 1: Configure KVM Target Servers*** (on page 14)
- ***Step 2: Configure Network Firewall Settings*** (on page 26)
- ***Step 3: Connect the Equipment*** (on page 27)
- ***Step 4: Configure the KX II*** (on page 29)
- ***Step 5 (Optional): Configure Keyboard Language*** (on page 35)

Also included in this section is the default login information you will need. Specifically, the default IP address, user name, and password. See ***Default Login Information*** (on page 13).

Default Login Information

Default	Value
User name	The default user name is admin. This user has administrative privileges.
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 KX II, you are required to change the default password.
IP address	The KX II ships with the default IP address of 192.168.0.192.

Important: 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.

Getting Started

Step 1: Configure KVM Target Servers

KVM target servers are the computers that will be accessed and controlled via the KX II. Before installing the 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 KX II remotely. See **Terminology** (on page 10) 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 KX II operates in several mouse modes:

- Absolute Mouse Mode™ (D2CIM-VUSB only)
- Intelligent Mouse Mode (do not use an animated mouse)
- Standard Mouse Mode

Mouse parameters do not have to be altered for Absolute Mouse Synchronization but D2CIM-VUSB or D2CIM-DVUSB is required for this mode. For both the Standard and Intelligent mouse modes, mouse parameters must be set to specific values, which are described here. 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 settings, see ***Intelligent Mouse Mode*** (on page 71).

Servers with internal KVM switches inside the blade chassis typically do not support absolute mouse technology.

Windows XP, Windows 2003 and Windows 2008 Settings

To configure KVM target servers running Microsoft® Windows XP® operating system, Windows 2003® operating system or Windows 2008® operating systems:

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 "Enhance 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.
3. Close the Control Panel.

Note: For KVM target servers running Windows XP, Windows 2000 or Windows 2008, you may wish to create a user name that will be used only for remote connections through the KX II. This will enable you to keep the target server's slow mouse pointer motion/acceleration settings exclusive to the KX II connection.

Windows XP, 2000, and 2008 login pages revert to preset mouse parameters that differ from those suggested for optimal 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 KX II mouse synchronization at the login pages by using the Windows registry editor to change the following settings: HKey_USERS\.DEFAULT\Control Panel\Mouse: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

Windows Vista Settings

To configure KVM target servers running Windows Vista® operating system:

1. Configure the mouse settings:
   a. Choose Start > Settings > Control Panel > Mouse.
   b. Select "Advanced system settings" from the left navigation panel. The System Properties dialog opens.
   c. Click the Pointer Options tab.
   d. 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 Performance Information then Tools > Advanced Tools > Adjust to adjust the appearance and performance of Windows.
   c. Click the Advanced tab.
   d. Click the Settings button in the Performance group to open the Performance Options dialog.
   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 and Close the Control Panel.

To configure KVM target servers running Windows 7® operating system:

1. Configure the mouse settings:
   a. Choose Start > Control Panel > Hardware and Sound > 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 Control Panel > System and Security.
   b. Select System and then select "Advanced system settings" from the left navigation panel. The System Properties dialog appears.
   c. Click the Advanced tab.
   d. Click the Settings button in the Performance group to open the Performance Options dialog.
   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 and Close the Control Panel.

Windows 2000 Settings

To configure KVM target servers running Microsoft® Windows 2000® operating system:

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.
      - Deselect the "Use the following transition effect for menus and tooltips" option.
3. Click OK and close the Control Panel.

Note: For KVM target servers running Windows XP, Windows 2000 or Windows 2008, you may wish to create a user name that will be used only for remote connections through the KX II. This will enable you to keep the target server's slow mouse pointer motion/acceleration settings exclusive to the KX II connection.

Windows XP, 2000, and 2008 login pages revert to preset mouse parameters that differ from those suggested for optimal 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 KX II mouse synchronization at the login pages by using the Windows registry editor to change the following settings: HKey_USERS\.DEFAULT\Control Panel\Mouse: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

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 the KX II.
   c. From the Advanced tab, verify that the Refresh Rate is supported by the 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 or /etc/X11/xorg.conf, depending on your X server distribution.

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 the 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-KX II supported resolutions.
   c. Disable the virtual desktop feature (not supported by the 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. Red Hat 5 users, choose Main Menu > Preferences > Mouse. Red Hat 4 users, choose System > Preferences > Mouse. The Mouse Preferences dialog appears.
   b. Click on 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 KX II.
   c. Click OK.

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 or /etc/X11/xorg.conf, depending on your X server distribution

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

SUSE Linux 10.1 Settings

Note: Do not attempt to synchronize the mouse at the SUSE Linux® 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 the KX II. See **Supported Video Resolutions** (on page 272) for more information.

   Note: If you change the video resolution, you must log out 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 System Menu > Preferences > Personal > Sessions.
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 out.
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 out, follow these procedures instead.

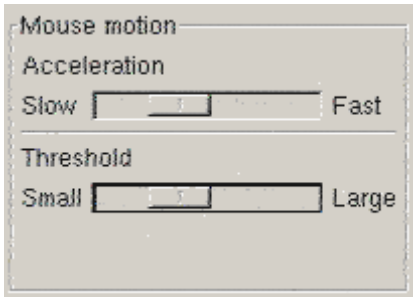
To make your settings permanent in Linux (no prompt):

1. Choose Desktop > Control Center > System > Sessions.
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 out.

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 the KX II. The most popular supported resolutions for Sun machines are:

Display resolution	Vertical refresh rate	Aspect ratio
1600 x 1200	60 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 out 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 out or restart computer.
64-bit	# /usr/sbin/m64config -prconf	1. # /usr/sbin/m64config -res 1024x768x75 2. Log out or restart computer.
32-bit and 64-bit	# /usr/sbin/fbconfig -prconf	1. # /usr/sbin/fbconfig -res 1024x768x75 2. Log out 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 KX II. See ***Supported Video Resolutions*** (on page 272) for more information.

Note: If you change the video resolution, you must log out 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 out.

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: 'USB Profile 'Mac OS-X, version 10.4.9 and later' must be selected from the USB Profile menu or the Port Configuration page.

Step 2: Configure Network Firewall Settings

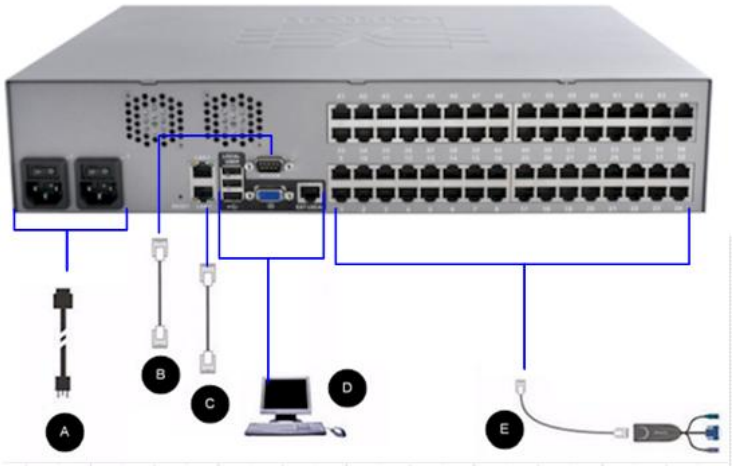
To access KX II through a network firewall via Multi-Platform Client or through the Port Access page, your firewall must allow communication on TCP Port 5000 or another port that you designate.

To take advantage of the 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

See ***Network Settings*** (on page 135) for additional information about designating another discovery port.

Step 3: Connect the Equipment

Connect the KX II to the power supply, network, local PC, local video display, keyboard and mouse, 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 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 KX II front panel will be red because the system is set to automatically detect both sources. See **Power Supply Setup** *(on page 157) for information about turning off automatic detection for the power source that is not in use.*

B. Modem Port (Optional)

The KX II features a dedicated modem port for remote access even when the LAN/WAN is unavailable. Using a straight-through serial (RS-232) cable, connect an external serial modem to the port labeled MODEM on the back of the KX II (see ***Specifications*** (on page 257) for a list of certified modems and ***Configuring Modem Settings*** (on page 148) for information on configuring the modem).

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

C. Network Port

The 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 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 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.

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

D. Local Access Port (Local Video Display, Keyboard and Mouse)

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

The KX2-832 and KX2-864 also provide you with an Extended Local port, labeled EXT LOCAL on the back of the device, for access to target servers while at the rack. The Extended Local port is not required for the initial installation and setup. It is configured from the Local Console and Remote Console.

To connect the local port:

- Attach a multi-sync VGA monitor, mouse, and keyboard to the respective Local User ports using a USB keyboard and mouse. The physical connections for the Local User and Extended Local ports can be found on the back panel of the KX II.

Connection	Description
Monitor	Attach a standard multi-sync VGA monitor to the HD15 (female) video

Connection	Description
	port.
Keyboard	Attach a standard USB keyboard to one of the USB Type A (female) ports.
Mouse	Attach a standard USB mouse to one of the USB Type A (female) ports.

E. Target Server Ports

The KX II uses standard UTP cabling (Cat5/5e/6) to connect to each target server.

To connect a target server to the KX II:

1. Use the appropriate Computer Interface Module (CIM). See Supported CIMs and Operating Systems (Target Servers) 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 KX II device.

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 4: Configure the KX II

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

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

Changing the Default Password

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

To change the default password:

1. Power on the KX II using the power switch(s) at the back of the unit. Wait for the KX II unit to boot. (A beep signals that the boot is complete.)
2. Once the unit has booted, the KX II Local Console is visible on the monitor attached to the 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 as well as special characters.
5. Click Apply.
6. 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, see **Network Settings**.

To assign an IP address:

1. Choose Device Settings > Network. The Network Settings page opens.
2. Specify a meaningful Device Name for your KX II device. Up to 32 alphanumeric characters using valid special characters and no spaces.
3. In the IPv4 section, enter or select the appropriate IPv4-specific network settings:
   a. Enter the IP Address if needed. The default IP address is 192.168.0.192.
   b. Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

c. Enter the Default Gateway if None is selected from the IP Auto Configuration drop-down.

d. Enter the Preferred DHCP Host Name if DHCP is selected from the IP Auto Configuration drop-down.

e. Select the IP Auto Configuration. The following options are available:

- None (Static IP) - This option requires that you manually specify the network parameters.

  This is the recommended option because the KX II is an infrastructure device and its IP address should not change.

- DHCP - Dynamic Host Configuration Protocol is used by networked computers (clients) to obtain unique IP addresses and other parameters from a DHCP server.

  With this option, network parameters are assigned by the DHCP server. If DHCP is used, enter the Preferred host name (DHCP only). Up to 63 characters.

4. If IPv6 is to be used, enter or select the appropriate IPv6-specific network settings in the IPv6 section:

   a. Select the IPv6 checkbox to activate the fields in the section.

   b. Enter a Global/Unique IP Address. This is the IP address assigned to the KX II.

   c. Enter the Prefix Length. This is the number of bits used in the IPv6 address.

   d. Enter the Gateway IP Address.

   e. Link-Local IP Address. This address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present. **Read-Only**

   f. Zone ID. This identifies the device with which the address is associated. **Read-Only**

   g. Select the IP Auto Configuration. The following options are available:

   - 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: Global/Unique IP Address, Prefix Length, and Gateway IP Address allowing you to manually set the IP configuration.

   - Router Discovery - Use this option to automatically assign IPv6 addresses that have Global or Unique Local significance beyond that of the Link Local, which only applies to a directly connected subnet.

5. Select Obtain DNS Server Address Automatically if DHCP is selected and Obtain DNS Server Address is enabled. When Obtain DNS Server Address Automatically, the DNS information provided by the DHCP server will be used.
6. If Use the Following DNS Server Addresses is selected, regardless of whether DHCP is selected or not, the addresses entered in this section will be used to connect to the DNS server.

   Enter the following information if the Following DNS Server Addresses option is selected. These addresses are the primary and secondary DNS addresses that will be used if the primary DNS server connection is lost due to an outage.

   a. Primary DNS Server IP Address

   b. Secondary DNS Server IP Address
7. When finished, click OK.

See ***LAN Interface Settings*** (on page 138) for information in configuring this section of the Network Settings page.

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 KX II LAN Interface Speed & Duplex field to 100 Mbps/Full Duplex (or whatever option is appropriate to your network) addresses the issue. See the **Network Settings** *(on page 135) 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. See **Step 3: Connect the Equipment** for a description of connecting the equipment.
2. Using the KX II Local Console, choose Device Settings > Port Configuration. The Port Configuration page opens.
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 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 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 enable automatic detection for the power supplies in use:

1. Choose Device Settings > Power Supply Setup. The Power Supply Setup page opens.
2. If you are plugging power input into power supply number one (left-most power supply at the back of the device), 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 device), select the PowerIn2 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 device turns red.

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

1. Using the 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, see ***Power Supply Setup*** (on page 157).

Note to CC-SG Users

If you are using the 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 help applies primarily to deploying the KX II device(s) without the integration functionality of CC-SG.

Remote Authentication

Note to CC-SG Users

When the 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 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 KX II. They will not be authenticated against the CC-SG user database.

For additional information about CC-SG authentication, see the CommandCenter Secure Gateway User Guide, Administrator Guide, or Deployment Guide, which can be downloaded from the Support section of the ***Raritan website http://www.raritan.com***.

Supported Protocols

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

Create User Groups and Users

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

The 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 KX II. This information is used to authenticate users attempting to access your KX II. See **User Management** for details on adding and editing user groups and users.

Step 5 (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.

Changing 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.

Chapter 3 Working with Target Servers

In This Chapter

Interfaces

There are several user interfaces in the KX II, providing you with easy access any time, anywhere. These include the KX II Local Console, the 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:

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

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

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

KX II Local Console Interface

When you are located at the server rack, the KX II provides standard KVM management and administration via the KX II Local Console. The 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. Additionally, the KX II provides terminal emulation when accessing serial targets.

There are many similarities among the KX II Local Console and the KX II Remote Console graphical user interfaces. Where there are differences, they are noted in the help.

The KX II Local Console Factory Reset option is available in the KX II Local Console but not the KX II Remote Console.

KX II Remote Console Interface

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

The KX II Remote Console provides a digital connection to your connected KVM target servers. When you log into a KVM target server using the KX II Remote Console, a Virtual KVM Client window opens.

There are many similarities among the KX II Local Console and the 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 KX II Remote Console but not the KX II Local Console:

- Virtual Media
- Favorites
- Backup/Restore
- Firmware Upgrade
- Upgrade Report
- SSL Certificates

Launching the KX II Remote Console

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

You can reduce the number of warning messages during subsequent log ins by checking the following options on the security and certificate warning messages:

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

To launch the KX II Remote Console:

1. Log in to any workstation with network connectivity to your KX II and Java Runtime Environment® installed (JRE® is available on the ***Java website http://java.sun.com/***).
2. Launch a supported web browser such as Internet Explorer® or Firefox®.
3. Type the following URL: *http://IP-ADDRESS*, where IP-ADDRESS is the IP address assigned to your KX II. You can also use https, the DNS name of the KX II assigned by the administrator (provided that a DNS server has been configured), or just simply type the IP address in the browser (KX II always redirects the IP address from HTTP to HTTPS.) The Login page opens.
4. Type your user name and password. If this is the first time logging in, log in with the factory default user name (admin) and password (raritan, all lower case). You will be prompted to change the default password. Click Login.

Note: If your administrator requires you read and/or accept a security agreement in order to access the device, a security banner will be displayed after you have entered your login credentials and clicked Login.

See ***Virtual KVM Client (VKC)*** (on page 51) for information on the KX II functions available via the Remote Console.

Interface and Navigation

KX II Console Layout

Both the KX II Remote Console and the 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. Three tabs are provided on the page allowing you to view by port, view by group or view by search. 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. See ***Port Access Page*** (on page 43) for more information.

Left Panel

The left panel of the KX II interface contains the following information. Note that some information is conditional and will only be displayed if you are a certain of user, are using certain features, and so on. This conditional information is noted here.

Information	Description	When displayed?
Time & Session	The date and time the current session started.	Always
User	Username	Always
State	The current state of the application, either idle or active. If idle, the application tracks and displays the time the session has been idle.	Always
Your IP	The IP address used to access the KX II.	Always
Last Login	The last login date and time.	Always
Under CC-SG Management	The IP address of the CC-SG device managing the KX II.	When the KX II is being managed by CC-SG.
Device Information	Information specific to the KX II you are using.	Always
Device Name	Name assigned to the device.	Always
IP Address	The IP address of the KX II.	Always
Firmware	Current version of firmware.	Always
Device Model	Model of the KX II	Always
Network	The name assigned to the current network.	Always
PowerIn1	Status of the power 1 outlet connection. Either on or off.	When connected.
PowerIn2	Status of the power 2 outlet connection. Either on or off.	When connected.

Information	Description	When displayed?
Configured As Base or Configured As Tiered	If you are using a tiering configuration, this indicates if the KX II you are accessing is the base device or a tiered device.	When the KX II is part of a tiered configuration.
Port States	The statuses of the ports being used by the KX II.	Always
Connect Users	The users, identified by their username and IP address, who are currently connected to the KX II.	Always
Help - User Guide	Links to online help.	Always
Favorite Devices	See ***Managing Favorites*** (on page 46).	Always
FIPS Mode	FIPS Mode: EnabledSSL Certificate: FIPS Mode Compliant	When FIPS is enabled.

KX II Console Navigation

The KX II Console interfaces 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 appears.
- Hover over a tab and select the appropriate option from the menu.
- Click the option directly from the menu hierarchy displayed (breadcrumbs).

To scroll through pages longer than the screen:

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

Port Access Page

After successfully logging on to the KX II Remote Console, the Port Access page appears. This page lists all of the 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 KX II. KVM target servers are servers that you want to control through the KX II device. They are connected to the KX II ports at the back of the device.

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

If you are using a tiered configuration in which a base KX II device is used to access multiple other tiered devices, the tiered devices are viewed on the Port Access page by clicking on the Expand Arrow icon ▶ to the left of the base device name. See ***Configuring and Enabling Tiering*** (on page 142) for more information on tiering.

Also displayed on the Port Access page are blade chassis that have been configured in the KX II. The blade chassis is displayed in an expandable, hierarchical list on the Port Access page, with the blade chassis at the root of the hierarchy and the individual blades labeled and displayed below the root. Use the Expand Arrow icon next to the root chassis to display the individual blades.

Note: To view the blade chassis in a hierarchal order, blade-chassis subtypes must be configured for the blade server chassis.

By default, the View by Port tab will be displayed on the Port Access page. The View by Group tab displays port groups and can be expandable to display ports that are assigned to the port group. The View by Search tab allows you to search by port name. The search feature supports the use of an asterisk (*) as a wildcard, and full and partial names.

▶ To use the Port Access page:

1. From the 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 KX II device. 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 KX II port. Initially, this is 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 appears.

Note: Do not use apostrophes for the Port (CIM) Name.

- Status - The status for standard servers is either up or down.
- Type - The type of server or CIM. For blade chassis, the type can be Blade Chassis, Blade, BladeChassisAdmin, and BladeChassisURL.

2. Click View by Port, View by Group or View by Search to switch between views.
3. Click the Port Name of the target server you want to access. The Port Action Menu appears. See **Port Action Menu** (on page 44) for details on available menu options.
4. Choose the desired menu command from the Port Action Menu.

To change the display sort order:

- Click the column heading by which you want to sort. 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 appears. Choose the desired menu option for that port to execute it. Note that only currently available options, depending on the port's status and availability, will be listed in the Port Action menu:

- Connect - Creates a new connection to the target server. For the KX II Remote Console, a new ***Virtual KVM Client*** (see "***Virtual KVM Client (VKC)***" on page 51) page appears. For the KX II Local Console, the display switches to the target server and switches away from the local user interface. On the local port, the KX II Local Console interface must be visible in order to perform the switch. Hot key switching is also available from the local port.

Note: This option is not available from the 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 KX II Local Console.

- Disconnect - Disconnects this port and closes the Virtual KVM Client page 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 KX II Local Console. The only way to disconnect from the switched target in the Local Console is to use the hot key.

- Power On - Powers on the target server through the associated outlet. This option is visible only when there are 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 are 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 are one or more power associations to the 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 Device Name, IP Address, or DNS hostname
- Discover KX II devices on its subnet (before and after login)
- Retrieve discovered KX II devices from the connected KX device (after login)

To access a favorite KX II device:

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

To display favorites by name:

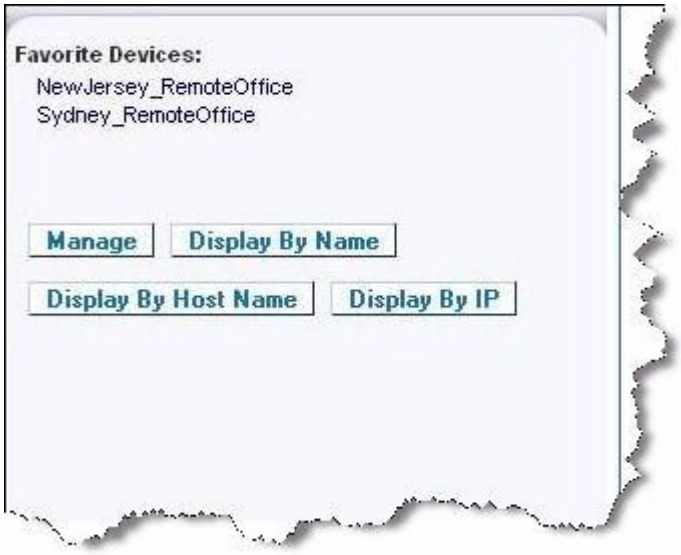
- Click Display by Name.

To display favorites by IP Address:

- Click Display by IP.

To display favorites by the host name:

- Click Display by Host Name.



Note: Both IPv4 and IPv6 addresses are supported.

Manage Favorites Page

To open the Manage Favorites page:

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

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

Favorites List Page

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.

Discovering Devices on the Local Subnet

This option discovers the devices on your local subnet, which is the subnet where the KX II Remote Console is running. These devices can be accessed directly from this page or you can add them to your list of favorites. See ***Favorites List Page*** (on page 47).

To discover devices on the local subnet:

1. Choose Manage > Discover Devices - Local Subnet. The Discover Devices - Local Subnet page appears.
2. Choose the appropriate discovery port:
   - To use the default discovery port, select the Use Default Port 5000 checkbox.
   - To use a different discovery port:
   a. Deselect the Use Default Port 5000 checkbox.
   b. Type the port number in 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.

Note: Both IPv4 and IPv6 addresses are supported.

Discovering Devices on the KX II Subnet

This option discovers devices on the device subnet, which is the subnet of the KX II device IP address itself. You can access these devices directly from this the Subnet page or add them to your list of favorites. See ***Favorites List Page*** (on page 47).

This feature allows multiple KX II devices to interoperate and scale automatically. The KX II Remote Console automatically discovers the KX II devices, and any other Raritan device, in the subnet of the KX II.

To discover devices on the device subnet:

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

To add devices to your Favorites List:

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

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

To access a discovered device:

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

Note: Both IPv4 and IPv6 addresses are supported.

Adding, Deleting and Editing Favorites

To add a device to your favorites list:

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

To edit a favorite:

1. From the Favorites List page, select the checkbox next to the appropriate KX II device.
2. Click the Edit button. The Edit page appears.
3. Update the fields as necessary:
   - Description
   - IP Address/Host Name - Type the IP address of the KX II device
   - Port (if necessary)
   - Product Type
4. Click OK.

To delete a favorite:

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

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

Note: Both IPv4 and IPv6 addresses are supported.

Logging Out

To quit the KX II Remote Console:

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

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

Proxy Server Configuration for use with MPC, VKC and AKC

When the use of a Proxy Server is required, a SOCKS proxy must also be provided and configured on the remote client PC.

Note: If the installed proxy server is only capable of the HTTP proxy protocol, you cannot connect.

To configure the SOCKS proxy:

1. On the client, select Control Panel > Internet Options.

a. On the Connections tab, click 'LAN settings'. The Local Area Network (LAN) Settings dialog opens.

b. Select 'Use a proxy server for your LAN'.

c. Click Advanced. The Proxy Settings dialog opens.

d. Configure the proxy servers for all protocols. IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

2. Click OK at each dialog to apply the settings.

3. Next, configure the proxies for Java™ applets by selecting Control Panel > Java.

e. On the General tab, click Network Settings. The Network Settings dialog opens.

f. Select Use Proxy Server.

g. Click Advanced. The Advanced Network Settings dialog opens.

h. Configure the proxy servers for all protocols. IMPORTANT: Do not select 'Use the same proxy server for all protocols'.

Note: The default port for a SOCKS proxy (1080) is different from HTTP proxy (3128).

4. If you are using standalone MPC, you must also do the following:

i. Open the start.bat file in MPC directory with a text editor.

j. Insert the following parameters to the command line. Add them before "-classpath": -DsocksProxyHost=<socks proxy ip addr> -DsocksProxyPort=<socks proxy port>

The parameters should look as follows:

```
start javaw -Xmn128M -Xmx512M -XX:MaxHeapFreeRatio=70
-XX:MinHeapFreeRatio=50 -Dsun.java2d.noddraw=true
-DsocksProxyHost=192.168.99.99 -DsocksProxyPort=1080
-classpath .\sdeploy.jar;.\sFoxtrot.jar;.\jaws.jar;.\sMpc.jar
com.raritan.rrc.ui.RRCApplication %1
```

Virtual KVM Client (VKC)

Please note this client is used by various Raritan products. As such, references to other products may appear in this section of help.

Overview

Whenever you access a target server using the Remote Console, a Virtual KVM Client (VKC) window opens. There is one Virtual KVM Client for each target server connected. 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 closes the Virtual KVM Client connection, so exercise caution.

Note: If you are using Firefox 3.0.3, you may experience problems launching the application. If this occurs, clear the browser cache and launch the application again.

Connecting to a KVM Target Server

To connect to a KVM target server:

1. From the 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 appears.
3. Click Connect. A Virtual KVM Client window opens to the target server connected to that port.

Toolbar

Button	Button Name	Description
	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).

Button	Button Name	Description
	Video Settings	Opens the Video Settings dialog, allowing you to manually adjust video conversion parameters.
	Color Calibration	Adjusts color settings to reduce excess color noise. Same as choosing Video > Color Calibrate. *Note: Not available in KX II-101-V2.*
	Target Screenshot	Click to take a screenshot of the target server and save it to a file of your choosing.
	Synchronize Mouse	Dual-mouse mode forces the realignment of the target server mouse pointer with the mouse pointer. *Note: Not available in KX II-101-V2.*
	Refresh Screen	Forces a refresh of the video screen.
	Auto-sense Video Settings	Forces a refresh of the video settings (resolution, refresh rate).
	Smart Card	Opens a dialog that allows you to select from a list of smart card readers connected to a client PC. *Note: This function is only available on the KSX II 2.3.0 or later, and the KX II 2.1.10 or later.*
	Send Ctrl+Alt+Del	Sends a Ctrl+Alt+Del hot key combination to the target server.
	Single Cursor Mode	Starts Single Cursor mode in which the local mouse pointer no longer appears onscreen. Press Ctrl+Alt+O to exit this mode. *Note: Not available in KX II-101-V2.*
	Full Screen Mode	Maximizes the screen real estate to view the target server desktop.
	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.

Switching Between KVM Target Servers

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

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

To switch between KVM target servers:

1. While already using a target server, access the KX II Port Access page.
2. Click the port name of the target you want to access. The Port Action menu appears.
3. Choose Switch From in 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.

To power cycle a KVM target server:

1. From the KX II Remote Console, click the Port Access tab. The Port Access page opens.
2. Click the Port Name of the appropriate target server. The Port Action menu appears.
3. Choose Power Cycle. A confirmation message appears.

To power on a target server:

1. From the KX II Remote Console, click the Port Access tab. The Port Access page opens.
2. Click the port name of the appropriate target server. The Port Action menu appears.
3. Choose Power On. A confirmation message appears.

To power off a target server:

1. From the 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 appears.
3. Choose Power Off. A confirmation message appears.

Disconnecting KVM Target Servers

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

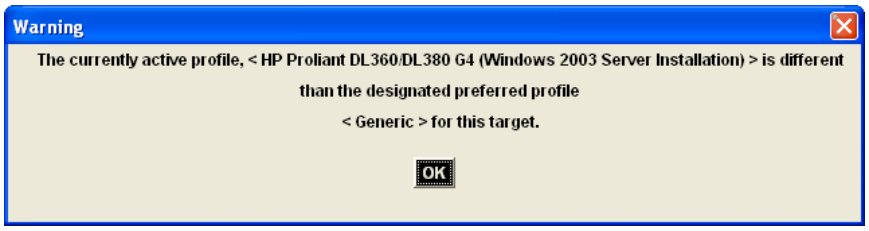
To disconnect a target server:

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

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 similar to the following:



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, based on your operational requirements. However, all profiles are available to be selected via the Other Profiles option on the USB Profile menu.

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 with which it should be used. See ***USB Profiles*** (on page 101) for details on USB profiles.

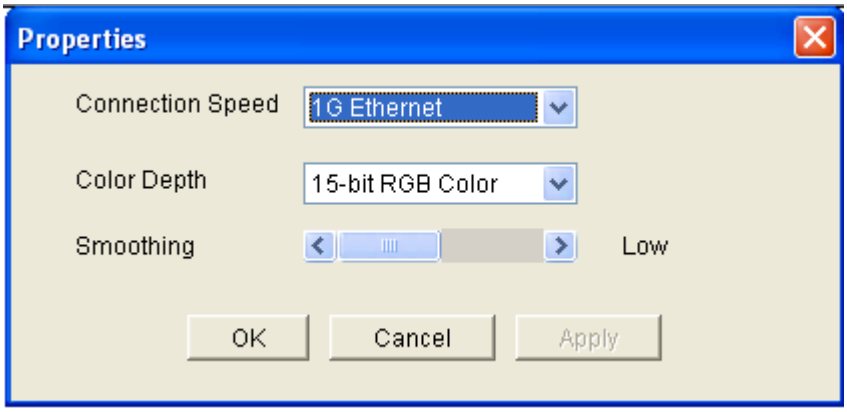
Connection Properties

The dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. The 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. Connection properties are saved across subsequent connections to generation 2 devices once they are set and saved.

To set the connection properties:

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



Note: KX II-101 does not support 1G Ethernet.

2. Choose the Connection Speed from the drop-down list. The device can automatically detect available bandwidth and not limit bandwidth use. However, 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)
- 56 kb (ISP Modem)
- 33 kb (Fast Modem)
- 24 kb (Slow Modem)

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 device 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, and so on), 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 > Info... The Connection Info window opens.

The following information is displayed about the current connection:

- Device Name - The name of the device.
- IP Address - The IP address of the 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.

Keyboard Options

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 cannot 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 Multi-Platform Client (MPC) and vice versa. However, keyboard macros created in Active KVM Client (AKC) cannot be used in VKC or MPC, and vice versa.

Note: KX II-101 does not support AKC.

Import/Export Keyboard Macros

Macros exported from Active KVM Client (AKC) cannot be imported into Multi-Platform Client (MPC) or Virtual KVM Client (VKC). Macros exported from MPC or VKC cannot be imported into AKC.

Note: KX II-101 does not support AKC.

To import macros:

1. Choose Keyboard > Import Keyboard Macros to open the Import Macros dialog. Browse to the folder location of the macro file.
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 is displayed and the import terminates once OK is selected.
   b. If the import fails, an error dialog appears and a message regarding why the import failed is displayed. 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 to begin the import.
   a. If a duplicate macro is found, the Import Macros dialog appears. Do one of the following:

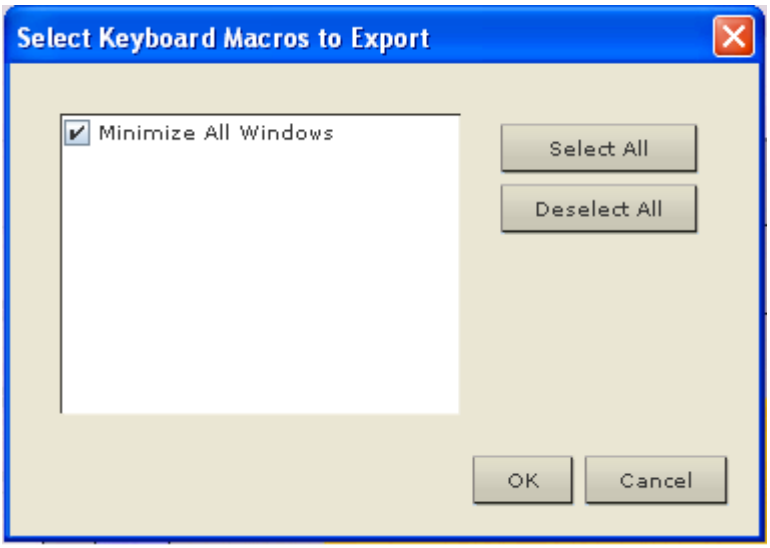
- Click Yes to replace the existing macro with the imported version.
- Click Yes to All to replace the currently selected and any other duplicate macros that are found.
- Click No to keep the original macro and proceed to the next macro
- Click No to All keep the original macro and proceed to the next macro. Any other duplicates that are found are 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 appears. Enter a new name for the macro in the field and click OK. The dialog closes and the process proceeds. If the name that is entered is a duplicate of a macro, an alert appears and you are required to enter another name for the macro.

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

The macros are then imported. If a macro is imported that contains a hot key that already exists, the hot key for the imported macro is discarded.

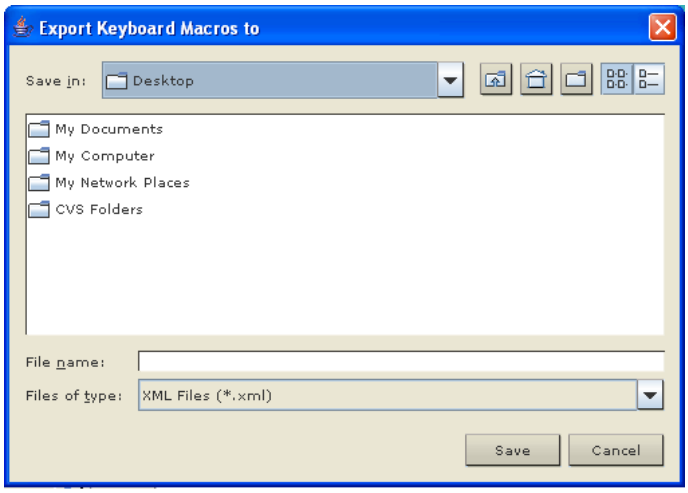
To export macros:

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 Export Keyboard Macro. A dialog from which to locate and select the macro file appears. By default, the macro exists on your desktop.
4. Select the folder to save the macro file to, enter a name for the file and click Save. If the macro already exists, you receive an alert message. Select Yes to overwrite the existing macro or No to close the alert without overwriting the macro.



Building a Keyboard Macro

To build a macro:

1. Click Keyboard > Keyboard Macros. The Keyboard Macros dialog appears.
2. Click Add. The Add Keyboard Macro dialog appears.
3. Type a name for the macro in the Keyboard Macro Name field. This name appears in the Keyboard menu after it is created.
4. 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**
5. In the Keys to Press drop-down list, select each key you would like to use to emulate the keystrokes that is used to perform the command. Select the keys in the order by which they are to be pressed. After each selection, select Add Key. As each key is selected, it appears in the Macro Sequence field and a Release Key command is automatically added after each selection.
6. To use the Send Text to Target function for the macro, click the Construct Macro from Text button.
7. For example, create a macro to close a window by selecting Left Ctrl + Esc. This appears in the Macro Sequence box as follows:

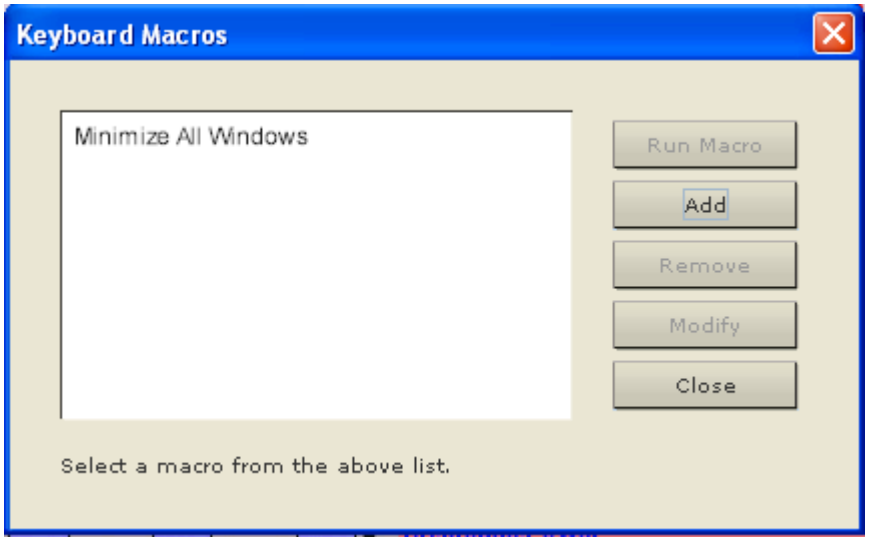
Press Left Ctrl

Release Left Ctrl

Press Esc

Release Esc

8. Review the Macro Sequence field to be sure the macro sequence is defined correctly.
   a. To remove a step in the sequence, select it and click Remove.
   b. 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.
9. 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.
10. Click Close to close the Keyboard Macros dialog. The macro now appears 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.



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.

Modifying and Removing Keyboard Macros

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.

Hot-key combinations that coincide with blade chassis switching key sequences will not be sent to blades housed in those chassis.

Setting CIM Keyboard/Mouse Options

To access the DCIM-USBG2 setup menu:

1. Put the mouse focus on a window such as Note Pad (Windows® operating system) or an equivalent.
2. Select Set CIM Keyboard/Mouse options. This is the equivalent of sending the Left-Control and Num Lock to the target. The CIM setup menu options are then displayed.

3. Set the language and mouse settings.
4. Exit the menu to return to normal CIM functionality.

Video Properties

Refreshing the 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  in the 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 the following:

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

Calibrating Color

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

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

Note: The KX II-101 does support color calibration.

To calibrate the color, do the following:

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

Adjusting Video Settings

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

To change the video settings:

1. Choose Video > Video Settings or click the Video Settings button  in the toolbar to open the Video Settings dialog.
2. Adjust the following settings as required. As you adjust the settings the effects are immediately visible:
   a. Noise Filter

      The device 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.

   b. PLL Settings

      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.

c. Brightness: Use this setting to adjust the brightness of the target server display.

d. Brightness Red - Controls the brightness of the target server display for the red signal.

e. Brightness Green - Controls the brightness of the green signal.

f. Brightness Blue - Controls the brightness of the blue signal.

g. Contrast Red - Controls the red signal contrast.

h. Contrast Green - Controls the green signal.

i. 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.

---

j. Horizontal Offset - Controls the horizontal positioning of the target server display on your monitor.

k. Vertical Offset - Controls the vertical positioning of the target server display on your monitor.

3. Select Automatic Color Calibration to enable this feature.
4. Select the video sensing mode:

   - Best possible video mode

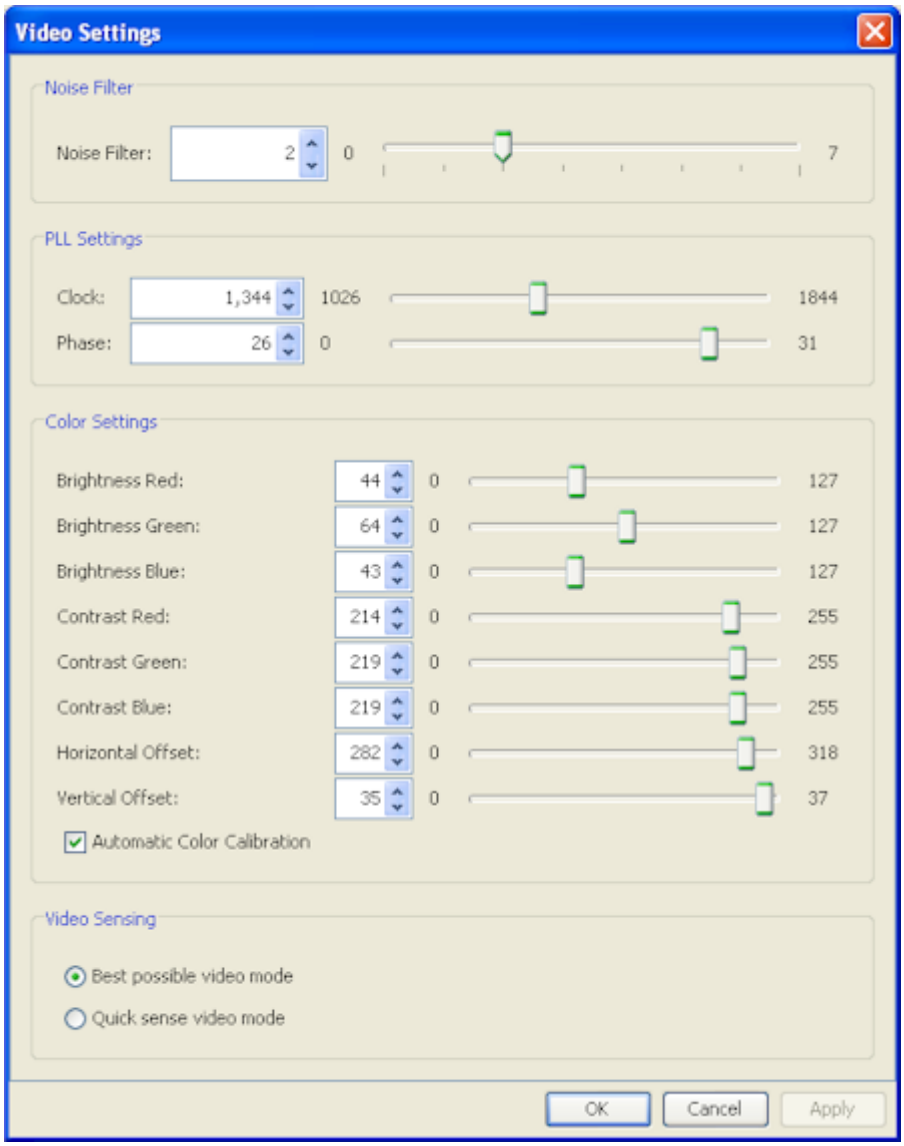
   The device will perform the full Auto Sense process when switching targets or target resolutions. Selecting this option calibrates the video for the best image quality.

   - Quick sense video mode

   With this option, the 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.

5. Click OK to apply the settings and close the dialog. Click Apply to apply the settings without closing the dialog.

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.

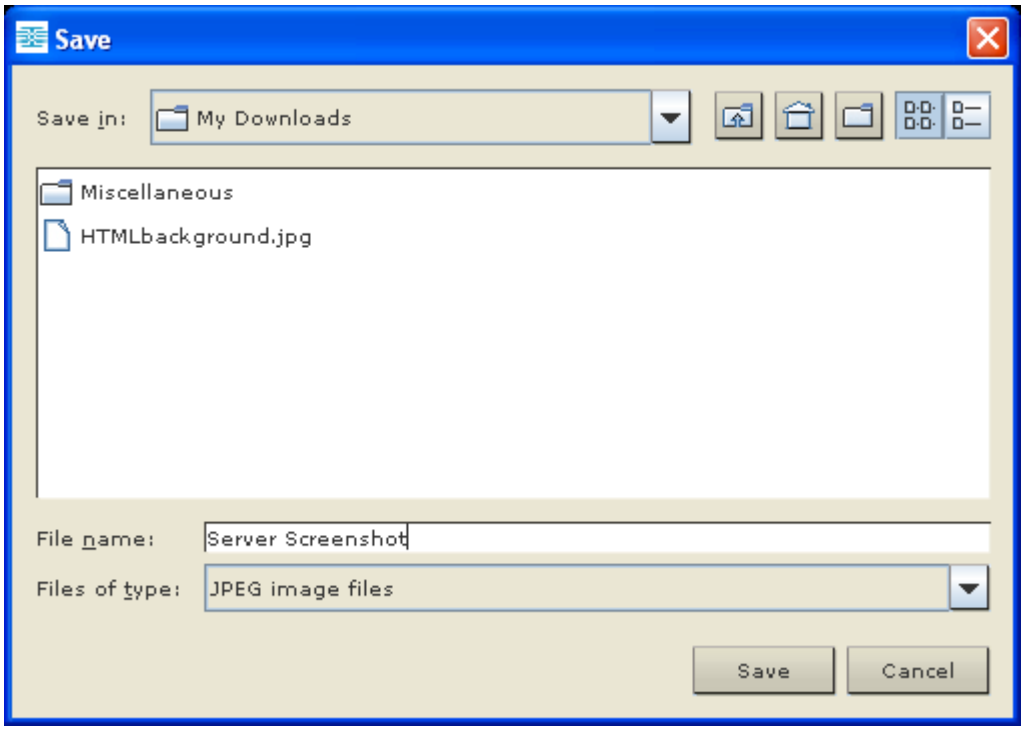


Using Screenshot from Target

You are able to take a screenshot of a target server using the Screenshot from Target server command. If needed, save this screenshot to a file location of your choosing as a bitmap, JPEG or PNG file.

To take a screenshot of the target server:

1. Select Video > Screenshot from Target or click the Screenshot from Target button  on the toolbar.
2. In the Save dialog, choose the location to save the file, name the file, and select a file format from the 'Files of type' drop-down.
3. Click Save to save the screenshot.



Changing the Maximum Refresh Rate

If the video card you are using on the target uses custom software and you are accessing the target through MPC or VKC, you may need to change the maximum refresh rate of the monitor in order for the refresh rate to take effect on the target.

To adjust the monitor refresh rate:

1. In Windows®, select Display Properties > Settings > Advanced to open the Plug and Play dialog.
2. Click on the Monitor tab.
3. Set the 'Screen refresh rate'.
4. Click OK and then OK again to apply the setting.

Mouse Options

When controlling a target server, the 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 align.

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

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

Mouse Pointer Synchronization

When remotely viewing a target server that uses a mouse, two mouse cursors are displayed: 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 can 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 are among those supported by the device. The Virtual KVM Client Connection Info dialog displays the actual values that the device is seeing.
2. For KX II devices, verify that the cable length is within the specified limits for the selected video resolution.
3. Verify that the mouse and video have been properly configured during the installation process.
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 or click the Synchronize Mouse button  in the toolbar.

Note: This option is available only in Standard and Intelligent mouse modes.

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.

To enter Standard Mouse mode:

- Choose Mouse > Standard.

Intelligent Mouse Mode

In Intelligent Mouse mode, the device can detect the target mouse settings and synchronize the mouse cursors accordingly, allowing mouse acceleration on the target. Intelligent mouse mode is the default for non-VM targets.

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

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

To enter absolute mouse mode:

- Choose Mouse > Absolute.

Note: The absolute mouse setting requires a USB target system and is the recommended mouse setting for KX II-101.

Note: For KX II devices, Absolute Mouse Synchronization is available for use with the virtual media-enabled USB CIM (D2CIM-VUSB and D2CIM-DVUSB) only.

Single Mouse Cursor

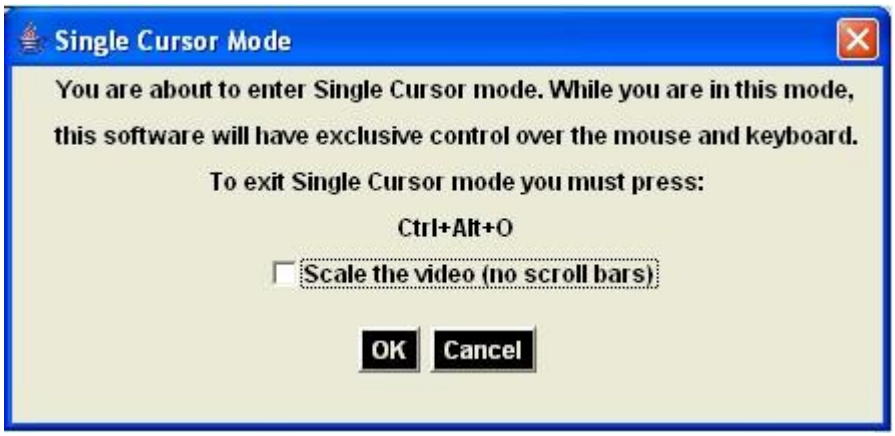
Single Mouse mode uses only the target server mouse cursor and the local mouse pointer no longer appears onscreen. While in single mouse mode, the Synchronize Mouse command is not available (there is no need to synchronize a single mouse cursor).

Note: VKC for the KX II-101 uses an icon set that differs from the icon set used in VKC for other Dominion KX products. See VKC Toolbar for the KX II-101 for additional information.

To enter single mouse mode, do the following:

1. Choose Mouse > Single Mouse Cursor.

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



To exit single mouse mode:

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

VKC Virtual Media

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

Smart Cards (VKC, AKC and MPC)

Using the KX II 2.1.10 or later, you are able to mount a smart card reader onto a target server to support smart card authentication and related applications. For a list of supported smart cards, smart card readers, and additional system requirements, see ***Supported and Unsupported Smart Card Readers*** (on page 275).

When accessing a server remotely, you will have the opportunity to select an attached smart card reader and mount it onto the server. Smart card authentication is used with the target server, it is not used to log into the device. Therefore, changes to smart card PIN and credentials do not require updates to device accounts. When mounted onto the target server, the card reader and smart card will cause the server to behave as if they had been directly attached. Removal of the smart card or smart card reader will cause the user session to be locked or you will be logged out depending on how the card removal policy has been setup on the target server OS. When the KVM session is terminated, either because it has been closed or because you switch to a new target, the smart card reader will be automatically unmounted from the target server.

When PC-Share mode is enabled on the device, multiple users can share access to a target server. However, when a smart card reader is connected to a target, the device will enforce privacy regardless of the PC-Share mode setting. In addition, if you join a shared session on a target server, the smart card reader mounting will be disabled until exclusive access to the target server becomes available.

After a KVM session is established to the target server, a Smart Card menu and button are available in the Virtual KVM Client (VKC), Active KVM Client (AKC) and Multi-Platform Client (MPC). Once the menu is opened or the Smart Card button is selected, the smart card readers that have been detected as attached to the remote client are displayed. From this dialog you can attach additional smart card readers, refresh the list of smart card readers attached to the target, and detach smart card readers. You are also able to remove or reinsert a smart card. This function can be used to provide notification to a target server OS that requires a removal/reinsertion in order to display the appropriate login dialog. Using this function allows the notification to be sent to a single target without affecting other active KVM sessions.

To mount a smart card reader:

1. Click the Smart Card menu and then select Smart Card Reader.

   Alternatively, click the Smart Card button  in the toolbar.
2. Select the smart card reader from the Select Smart Card Reader dialog.
3. Click Mount.

4. A progress dialog will open. Check the 'Mount selected card reader automatically on connection to targets' checkbox to mount the smart card reader automatically the next time you connect to a target. Click OK to begin the mounting process.

To update the smart card in the Select Smart Card Reader dialog:

- Click Refresh List if a new smart card reader has been attached to the client PC.

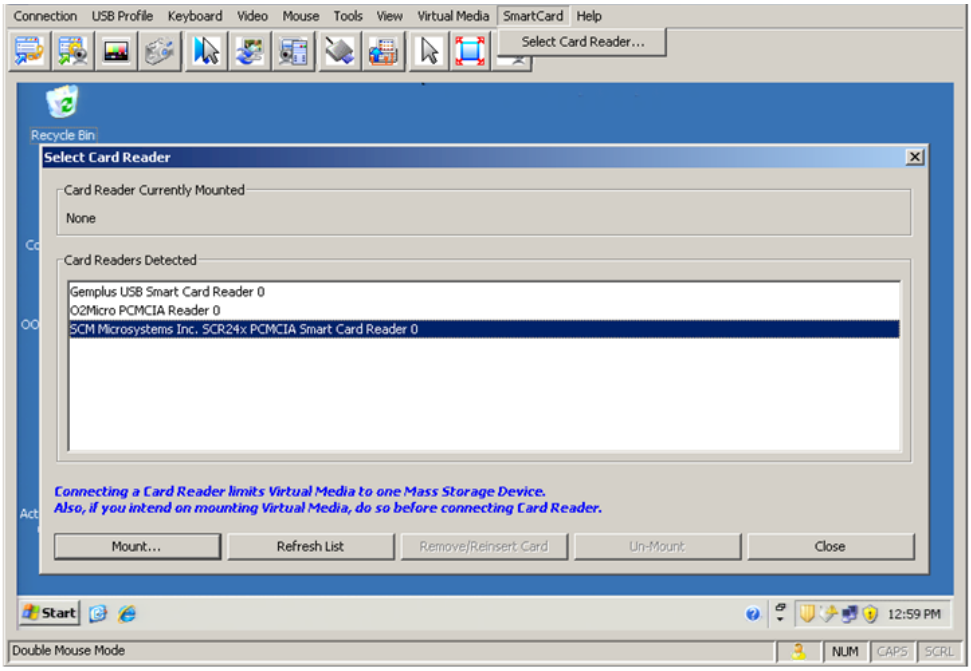
To send smart card remove and reinsert notifications to the target:

- Select the smart card reader that is currently mounted and click the Remove/Reinsert button.

To unmount a smart card reader:

- Select the smart card reader to be unmounted and click the Unmount button.

Smart card reader mounting is also supported from the Local Console. See **Local Console Smart Card Access** (on page 244) in your Dominion device help.



Tool Options

From the Tools menu, you can specify certain options for use with the Virtual KVM Client, including logging, setting the keyboard type, and defining hot keys for exiting Full Screen mode and Single Cursor mode.

Note: The KX II-101 and KX II-101-V2 do not support single cursor mode.

To set the tools options:

1. Choose Tools > Options. The Options dialog appears.
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)
   - French (Belgium)
   - Norwegian (Norway)
   - Portuguese (Portugal)
   - Danish (Denmark)
   - Swedish (Sweden)
   - German (Switzerland)
   - Hungarian (Hungary)
   - Spanish (Spain)
   - Italian (Italy)
   - Slovenian
   - Translation: French - US
   - Translation: French - US International

Note: In AKC, the keyboard type defaults to the local client, so this option does not apply.

Note: The KX II-101 does not support AKC.

4. Exit Full Screen Mode - Hotkey. When you enter Full Screen 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. Click OK.

Client Launch Settings

KX II users can also configure client launch settings that allow you to define the size of the screen for a KVM session.

6. Select the Client Launch Settings tab.
   a. To configure the target window settings:
   - Select 'Standard - sized to target Resolution' to open the window using the target's current resolution. If the target resolution is greater than the client resolution, the target window covers as much screen area as possible and scroll bars are added (if needed).
   - Select Full Screen to open the window in full screen mode.

   a. To configure the monitor on which the target viewer is launched:
   - Select 'Monitor Client Was Launched from' if you want the target viewer to be launched using the same display as the application that is being used on the client (for example, a web browser or applet).
7. Use Select From Detected Monitors to select from a list of target monitors that are currently detected by the application. If a previously selected monitor is no longer detected, 'Currently Selected Monitor Not Detected' is displayed.
8. Click OK.

Keyboard Limitations

Slovenian Keyboards

The < key does not work on Slovenian keyboards due to a JRE limitation.

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

Language	Configuration method
French	Keyboard Indicator
German	System Settings (Control Center)
Japanese	System Settings (Control Center)
UK	System Settings (Control Center)
Korean	System Settings (Control Center)
Belgian	Keyboard Indicator
Norwegian	Keyboard Indicator
Danish	Keyboard Indicator
Swedish	Keyboard Indicator
Hungarian	System Settings (Control Center)
Spanish	System Settings (Control Center)
Italian	System Settings (Control Center)
Slovenian	System Settings (Control Center)
Portuguese	System Settings (Control Center)

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

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 Full Screen mode, the target's full screen is displayed 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). While in Full Screen mode, moving your mouse to the top of the screen will display the Full Screen mode menu bar.

To enter full screen mode:

- Choose View > Full Screen.

To exit full screen mode:

- Press the hot key configured in the Tools Options dialog. The default is Ctrl+Alt+M. For AKC, select Connection/Exit from the hidden menu bar, which is accessed by hovering your mouse at the top of the screen.

Note: KX II-101 does not support AKC.

Alternatively, if you want to access the target in full screen mode at all times, you can make Full Screen mode the default.

To set Full Screen mode as the default mode:

1. Click Tools > Options to open the Options dialog.
2. Select Enable Launch in Full Screen Mode and click OK.

Help Options

About Raritan Virtual KVM Client

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

To obtain version information:

1. Choose Help > About Raritan Virtual KVM Client.
2. Use the Copy to Clipboard button to copy the information contained in the dialog to a clipboard file so it can be accessed later when dealing with support (if needed).

Active KVM Client (AKC)

Please note this client is used by various Raritan products. As such, references to other products may appear in this section of help.

Overview

The Microsoft Windows .NET-based Active KVM Client (AKC) is available with the KX II 2.2 (or later) and supports all KX II models, although the KX2-101 is not currently supported. AKC is based on Microsoft Windows .NET technology and allows users to run the client in Windows environments without the use of the Java Runtime Environment (JRE), which is required to run Raritan's Virtual KVM and Multi-Platform clients. AKC also works with CC-SG.

AKC and VKC share similar features with the exception of the following:

- Minimum system requirements
- Supported operating systems and browsers
- Keyboard macros created in AKC cannot be used in VKC.

See the **Virtual KVM Client (VKC)** (on page 51) section for information on using the available features of the application. If there is a difference between how AKC functions as compared to VKC, it is noted in the topic.

Also see ***Enabling Direct Port Access*** (see "***Enabling Direct Port Access via URL***" on page 146)and ***Enabling the AKC Download Server Certificate Validation*** (on page 147) for configuration information on using AKC.

Note: If you are using direct port access with AKC, you must open a new browser window or browser tab for each target you want to access. If you try to access another target by entering the DPA URL into the same browser window or browser tab you are currently accessing a target from, you will not be able to connect and may receive an error.

AKC Supported Operating Systems and Browsers

.NET Framework

AKC requires Windows .NET® version 3.5, and will work with both 3.5 and 4.0 installed.

Operating Systems

When launched from Internet Explorer®, AKC allows you to reach target servers via the KX II 2.2 (or later). AKC is compatible with the following platforms running .NET Framework 3.5:

- Windows XP® operating system
- Windows Vista® operating system (up to 64 bit)
- Windows 7® operating system (up to 64 bit)

Note: You must be using Windows 7 if WINDOWS PC FIPs is turned on and you are accessing a target using AKC and a smartcard.

Since .NET is required to run AKC, if you do not have .NET installed or you have an unsupported version of .NET installed, you will receive a message instructing you to check the .NET version.

Browser

- Internet Explorer 6 or later

If you attempt to open AKC from a browser other than IE 6 or later, you will receive an error message instructing you to check your browser and to switch to Internet Explorer.

Prerequisites for Using AKC

In order to use AKC:

- Ensure the cookies from the IP address of the device that is being accessed are not currently being blocked.
- Windows Vista, Windows 7 and Windows 2008 server users should ensure that the IP address of the device being accessed is included in their browser's Trusted Sites Zone and that Protected Mode is not on when accessing the device.

Enable AKC Download Server Certificate Validation

If the device (or CC-SG) administrator has enabled the Enable AKC Download Server Certificate Validation option:

- Administrators must upload a valid certificate to the device or generate a self-signed certificate on the device. The certificate must have a valid host designation.
- Each user must add the CA certificate (or a copy of self-signed certificate) to the Trusted Root CA store in their browser.

When launching AKC from the CC-SG Admin Client, you must have JRE™ 1.6.0_10 or above.

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. For details on using MPC, see the **KVM and Serial Access Clients Guide** available on Raritan's website on the same page as the user guide. Instructions on launching MPC are provided there.

Please note this client is used by various Raritan products. As such, references to other products may appear in this section of help.

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.

Important: Only Mac 10.5 and 10.6 with an Intel® processor can run JRE 1.6 and, therefore, be used as a client. Mac 10.5.8 does not support MPC as a standalone client.

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 opens in a new window.

Note: The Alt+Tab command toggles 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.

Note: If you are using Firefox 3.0.3, you may experience problems launching the application. If this occurs, clear the browser cache and launch the application again.

Chapter 4 Rack PDU (Power Strip) Outlet Control

In This Chapter

Overview

The KX II allows you to control Raritan PX and RPC series rack PDU (power strip) outlets connected to the KX II through a D2CIM-PWR.

Once a PX or RPC series is setup and then attached to the KX II, the rack PDU and its outlets can be controlled from the Powerstrip page in the KX II interface. This page is accessed by clicking on the Power menu at the top of the page.

The Powerstrip page will display rack PDUs attached to the KX II for which the user has been granted appropriate port access permissions. In the case of tiered configurations, the Powerstrip page will display both rack PDUs attached to the base and tiered KX IIs, for which the user has been granted appropriate port access permissions.

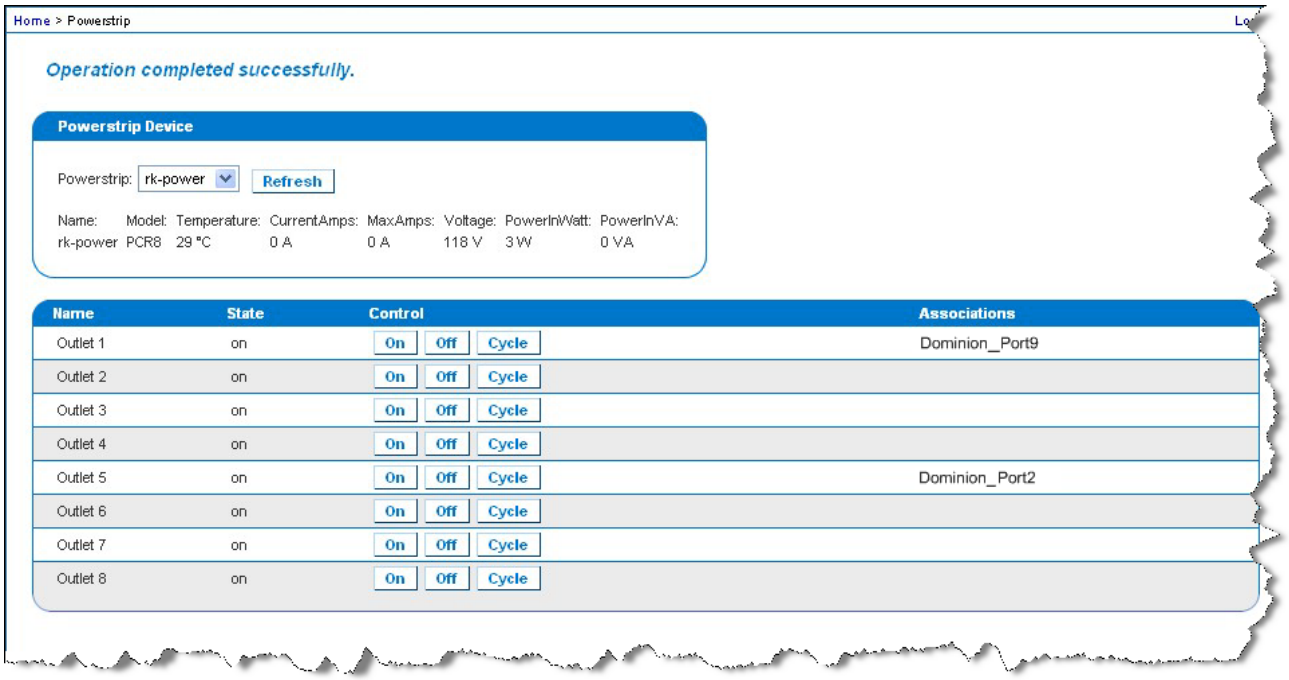
*Note: For information on setting up a PX, see the **Dominion PX User Guide**.*

From the Powerstrip page, you are able to turn the outlets on and off, as well as cycle their power. You are also able to view the following power strip and outlet information:

- Powerstrip Device Information:
  - Name
  - Model
  - Temperature
  - Current Amps
  - Maximum Amps
  - Voltage
  - Power in Watts
  - Power in Volts Ampere
- Outlet Display Information:
  - Name - Named assigned to the outlet when it was configured.
  - State - On or Off status of the outlet.

- Control - Turn outlets on or off, or cycle their power.
- Association - The ports associated with the outlet.

Initially, when you open the Powerstrip page, the power strips that are currently connected to the KX II are displayed in the Powerstrip drop-down. Additionally, information relating to the currently selected power strip is displayed. If no power strips are connected to the KX II, a message stating "No powerstrips found" will be displayed in the Powerstrip Device section of the page.

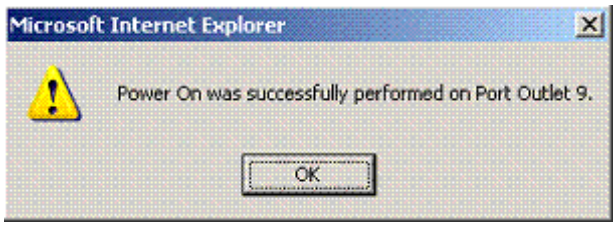


Turning Outlets On/Off and Cycling Power

To turn an outlet on:

1. Click the Power menu to access the Powerstrip page.
2. From the Powerstrip drop-down, select the PX rack PDU (power strip) you want to turn on.
3. Click Refresh to view the power controls.
4. Click On.

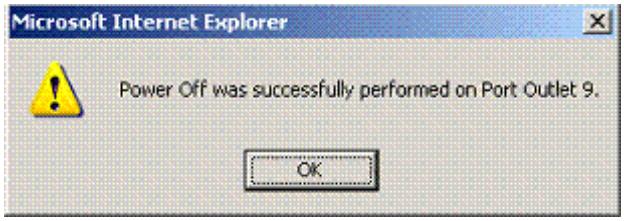
5. Click OK to close the Power On confirmation dialog. The outlet will be turned on and its state will be displayed as 'on'.



To turn an outlet off:

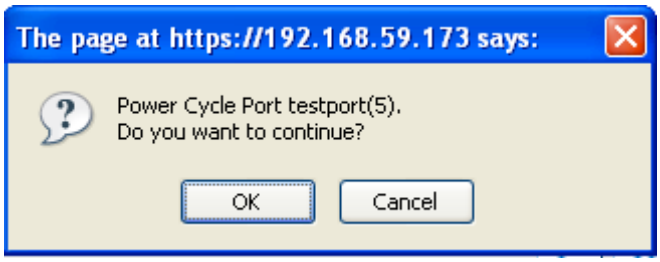
1. Click Off.
2. Click OK on the Power Off dialog.

3. Click OK on the Power Off confirmation dialog. The outlet will be turned off and its state will be displayed as 'off'.

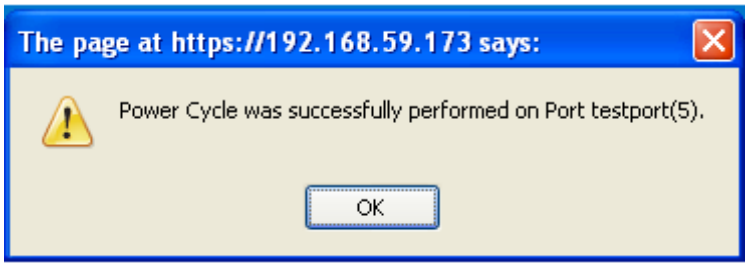


To cycle the power of an outlet:

1. Click the Cycle button. The Power Cycle Port dialog opens.



2. Click OK. The outlet will then cycle (note that this may take a few seconds).



3. Once the cycling is complete the dialog will open. Click OK to close the dialog.

Chapter 5 Virtual Media

In This Chapter

Overview

Virtual media extends KVM capabilities by enabling KVM target servers to remotely access media from a client PC and network file servers. With this feature, media mounted on a 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. In addition to data file support via virtual media files are supported by virtual media via a USB connection.

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.

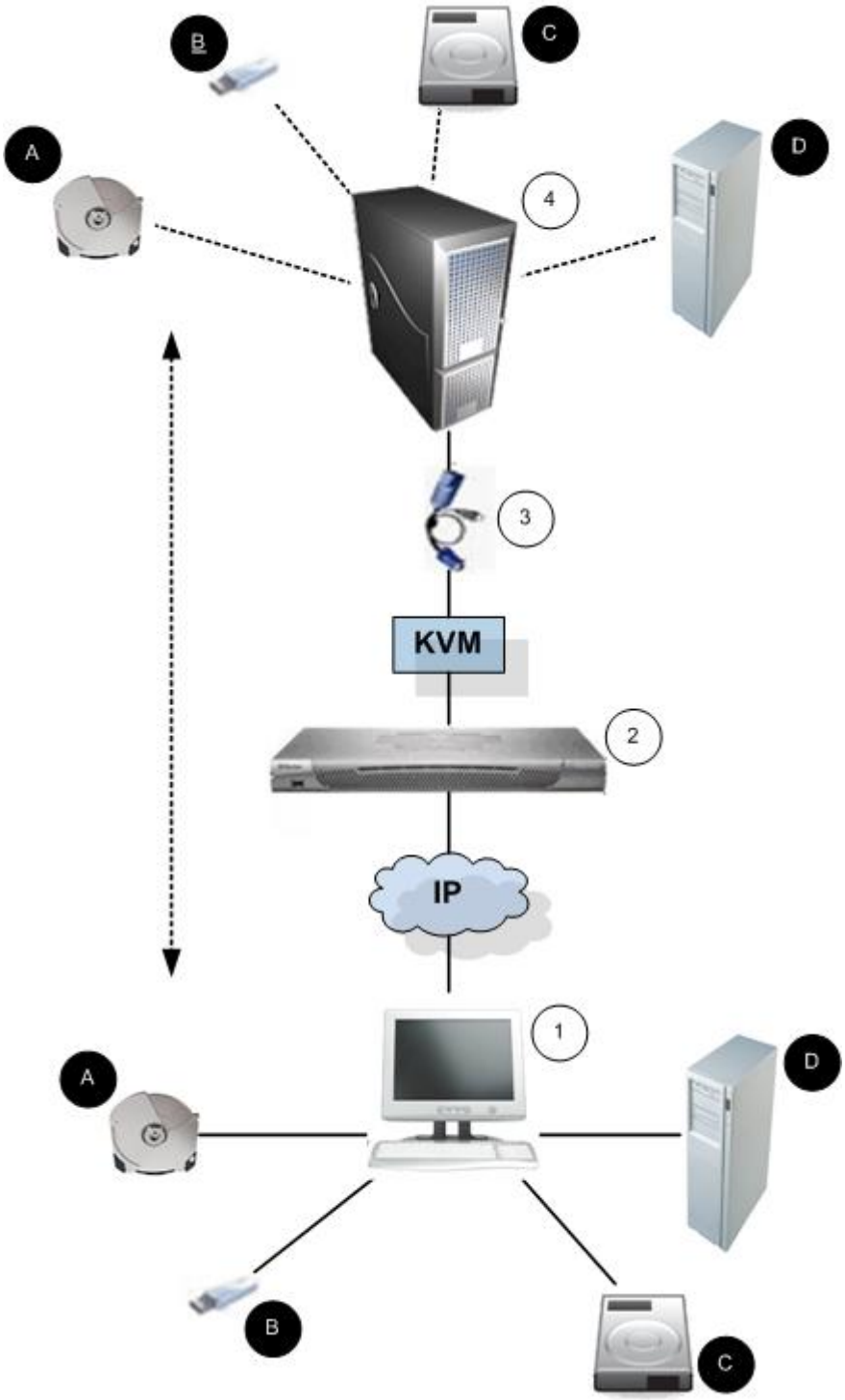


Diagram key			
1	Desktop PC	A	CD/DVD drive
2	KX II	B	USB mass storage device
3	CIM	C	PC hard drive
4	Target server	D	Remote file server (ISO images)

Prerequisites for Using Virtual Media

With the 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, 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.

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

Dominion Device

- For users requiring access to virtual media, the device 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.
- A USB connection must exist between the device and the target server.
- If you want to use PC-Share, Security Settings 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 or Windows 7, disable User Account Control or select Run as Administrator when starting Internet Explorer. To do this, click the Start Menu, locate IE, right-click 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.

Using Virtual Media via VKC and AKC in a Windows Environment

Windows XP® operating system administrator and standard user privileges vary from those of the Windows Vista® operating system and the Windows 7® operating system.

When enabled in Vista or Windows 7, User Access Control (UAC) provides the lowest level of rights and privileges a user needs for an application. For example, a Run as Administrator option is provided for Internet Explorer® for Administrator level tasks; otherwise these are not be accessible even though the user has an Administrator login.

Both of these features affect the types of virtual media that can be accessed by users via Virtual KVM Client (VKC) and Active KVM Client (AKC). See your Microsoft® help for additional information on these features and how to use them.

Following is a list virtual media types users can access via VKC and AKC when running in a Windows environment. The features are broken down by client and the virtual media features that are accessible to each Windows user role.

Windows XP

If you are running VKC and AKC in a Windows XP environment, users must have Administrator privileges to access any virtual media type other than CD-ROM connections, ISOs and ISO images.

Windows Vista and Windows 7

If you are running VKC and AKC in a Windows Vista or Windows 7 environment and UAC is enabled, the following virtual media types can be accessed depending on the user's Windows role:

Client	Administrator	Standard User
AKC and VKC	Access to: • Fixed drives and fixed drive partitions • Removable drives • CD/DVD drives • ISO images • Remote ISO images	Access to: • Removable drives • CD/DVD drives • ISO images • Remote ISO images

Using Virtual Media

See Prerequisites for Using Virtual Media before proceeding with using virtual media.

To use virtual media:

1. If you plan to access file server ISO images, identify those file servers and images through the Remote Console File Server Setup page. See File Server Setup (File Server ISO Images Only).

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

2. Open a KVM session with the appropriate target server.
   a. Open the Port Access page from the 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 window.

3. Connect to the virtual media.

For:	Select this VM option:
Local drives	Local Drives
Local CD/DVD drives	CD-ROM/DVD-ROM/ISO Images
ISO Images	Connect CD-ROM/ISO Image
File Server ISO Images	Connect CD-ROM/ISO Image

Upon completion of your tasks, disconnect the virtual media. See ***Disconnecting Virtual Media*** (on page 100).

File Server Setup (File Server ISO Images Only)

Note: This feature is only required when using virtual media to access file server ISO images. ISO9660 format is the standard supported by Raritan. However, other CD-ROM extensions may also work.

Note: SMB/CIFS support is required on the file server.

Use the Remote Console File Server Setup page to designate the files server(s) and image paths that you want to access using virtual media. File server ISO images specified here are 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 99).

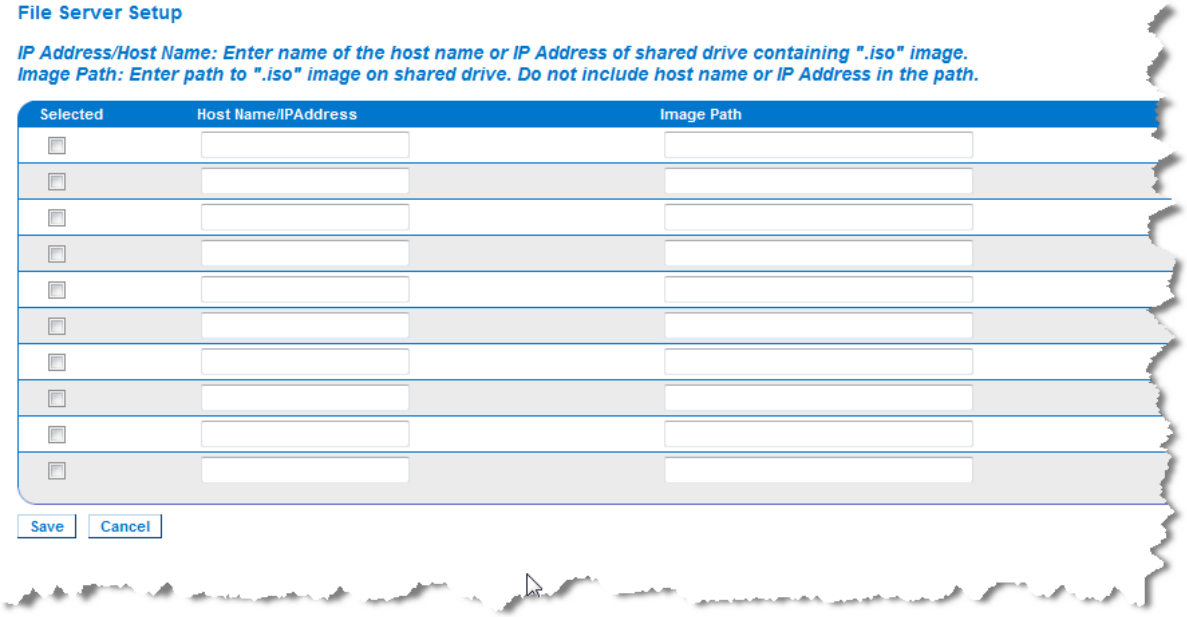
To designate file server ISO images for virtual media access:

1. Choose Virtual Media from the Remote Console. The File Server Setup page opens.
2. Check the Selected checkbox for all media that you want accessible as virtual media.
3. Enter information about the file server ISO images that you want to access:
   - IP Address/Host Name - Host name or IP address of the file server.
   - Image Path - Full path name of the location of the ISO image. For example, /sharename0/path0/image0.iso, \sharename1\path1\image1.iso, and so on.

   Note: The host name cannot exceed 232 characters in length.
4. Click Save. All media specified here are now available for selection in the Map Virtual Media CD/ISO Image dialog.

Note: You cannot access a remote ISO image via virtual media using an IPv6 address due to technical limitations of third-party software used by the by the KX, KSX or KX101 G2 device.

Note: If you are connecting to a Windows 2003® server and attempt to load an ISO image from the server, you may receive an error stating "Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password". If this occurs, disable "Microsoft Network Server: Digitally Sign Communications".



Note: You cannot access a remote ISO image via virtual media using an IPv6 address due to technical limitations of third-party software used by the KX2.

Note: If you are connecting to a Windows 2003 Server and attempt to load an ISO image from the server, you may receive an error stating "Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password". If this occurs, disable the "Microsoft Network Server: Digitally Sign Communications" option on the server under the Domain Controllers policies.

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.

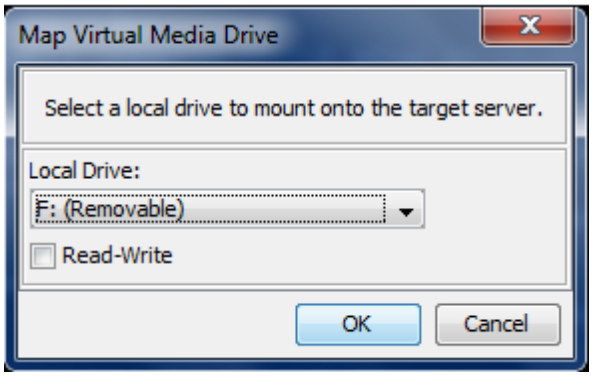
If this occurs, close the Remote Console and reconnect before redirecting another virtual media device. If other users are connected to the same target server, they must also close their connections to the target server.

Note: In the KX II 2.3.0 and above, when you mount an external drive such as a floppy drive, the LED light on the drive will remain on because the device is checking the drive every 500 milliseconds to verify the drive is still mounted.

Note: In the Dominion KX II 2.1.0 and above, when you mount an external drive, such as a floppy drive, the LED light on the drive will remain on because the device is checking the drive every 500 milliseconds to verify the drive is still mounted.

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.



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. See the ***Conditions when Read/Write is Not Available*** (on page 98) 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.

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.

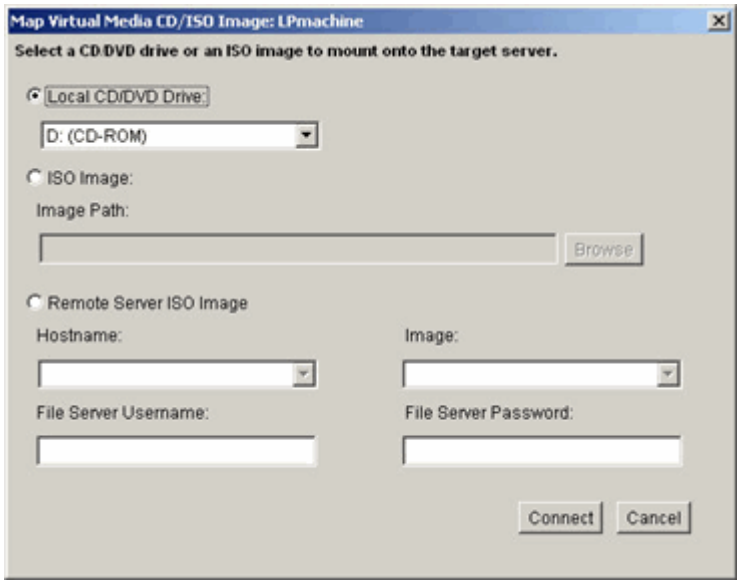
CD-ROM/DVD-ROM/ISO Images

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.



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 list. The file servers and image paths available are those that you configured using the File Server Setup page. Only items you configured using the File Server Setup page will be in the drop-down list.
   c. File Server Username - User name required for access to the file server. The name can include the domain name such as mydomain/username.
   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.

Note: If you are using the Windows 7® operating system®, Removable Disk is not displayed by default in the Window's My Computer folder when you mount a Local CD/DVD Drive or Local or Remote ISO Image. To view the Local CD/DVD Drive or Local or Remote ISO Image in this folder, select Tools > Folder Options > View and deselect "Hide empty drives in the Computer folder".

Note: You cannot access a remote ISO image via virtual media using an IPv6 address due to technical limitations of third-party software used by the KX II.

Note: You cannot access a remote ISO image via virtual media using an IPv6 address due to technical limitations of third-party software used by the KX2.

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 6 USB Profiles

In This Chapter

Overview

To broaden the 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 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*** (see "***Virtual KVM Client (VKC)***" on page 51), 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, please contact Raritan Technical Support for assistance.

CIM Compatibility

In order to make use of USB profiles, you must use a D2CIM-VUSB or D2CIM-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 KX II firmware upgrade, but VM-CIMs that have not had their firmware upgraded can be upgraded as described in ***Upgrading CIMs*** (on page 217).

See Computer Interface Modules (CIMs) for additional information.

Available USB Profiles

The current release of the 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. As new profiles are added, they will be documented in the help.

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
BIOS Dell OptiPlex ™ 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 profile	Description
	• USB bus speed limited to full-speed (12 MBit/s) • No virtual media support
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
BIOS ASUS P4C800 Motherboard	Use this profile to access BIOS and boot from Virtual Media on Asus P4C800-based systems. Restrictions: • USB bus speed limited to full-speed (12 MBit/s) • Virtual CD-ROM and disk drives cannot be used simultaneously

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 HP Compaq® 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
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
IBM BladeCenter H with	Use this profile to enable virtual media

USB profile	Description
Advanced Management Module	functionality when D2CIM-VUSB or D2CIM-DVUSB is connected to the Advanced Management Module. Restrictions: • 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® operating system, Windows XP® operating system, Windows Vista® operating system and later. Restrictions: • None
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	HP Proliant DL360/DL380 G4

USB profile	Description
Installation)	(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 distributions. Restrictions: • Absolute mouse synchronization™ not supported
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

USB profile	Description
	series mainboards with Phoenix AwardBIOS. Restrictions: • Virtual CD-ROM and disk drives cannot be used simultaneously
Suse 9.2	SuSE Linux 9.2 Use this for SuSE Linux 9.2 distribution. 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.
Troubleshooting 3	Troubleshooting Profile 3 • Mass Storage first • Keyboard and Mouse (Type 2)

USB profile	Description
	• 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 KX II comes with a set of USB profiles that you can 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 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, AKC and 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. If required, the user can select a USB profile from the USB Profile menu in VKC, AKC or MPC.

For information about assigning USB profiles to a KVM port, see ***Configuring USB Profiles (Port Page)*** (on page 187).

Mouse Modes when Using the Mac OS-X USB Profile with a DCIM-VUSB

If you are using a DCIM-VUSB, using a Mac OS-X® USB profile, and running Mac OS-X 10.4.9 (or later), when you reboot you must be in Single Mouse mode to use the mouse at the Boot menu.

To configure the mouse to work at the Boot menu:

1. Reboot the Mac and press the Option key during the reboot to open the Boot menu. The mouse will not respond at this point.
2. Select Intelligent Mouse mode and then select Single Mouse mode. The mouse will respond.

   Note: Mouse speed may be slow while in Single Mouse mode.

3. Once you are out of the Boot menu and have booted to the operating system, exit Single Mouse mode and switch back to Absolute Mouse mode for better mouse performance.

Chapter 7 User Management

In This Chapter

User Groups

The 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 KX II is configured for LDAP/LDAPS or RADIUS, that authentication is processed first, followed by local authentication.

Every 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.

Up to 254 user groups can be created in the KX II. Up to 254 user groups can be created in the KX II.

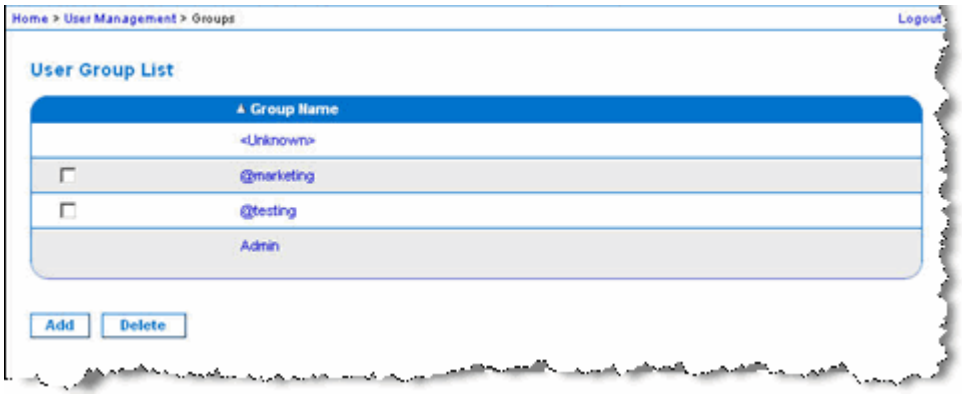
User Group List

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.



Relationship Between Users and Groups

Users belong to a group and groups have privileges. Organizing the various users of your 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.

Adding a New User Group

To add a new user group:

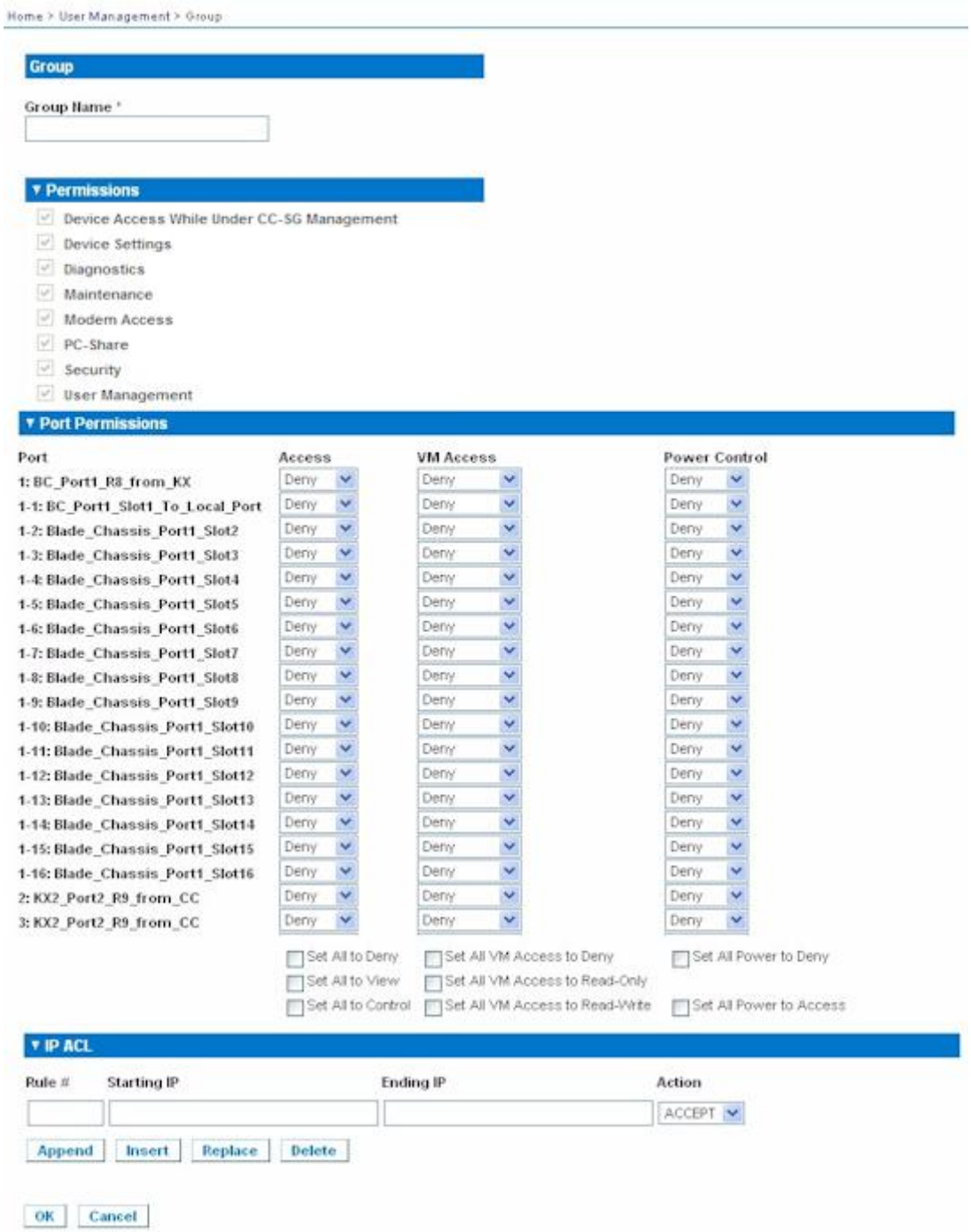
1. Open the Group page by selecting User Management > Add New User Group or clicking the Add button from the User Group List page.

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 (up to 64 characters).
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. See ***Setting Permissions*** (on page 114).
4. Set the port permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). See ***Setting Port Permissions*** (on page 115).
5. Set the IP ACL. This feature limits access to the KX II device by specifying IP addresses. It 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 (and takes priority). **Optional**. See ***Group-Based IP ACL (Access Control List)*** (on page 116).
6. Click OK.

Note: Several administrative functions are available within MPC and from the KX II Local Console. These functions are available only to members of the default Admin group.

Note: Both IPv4 and IPv6 addresses are supported.



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 Access While Under CC-SG Management	Allows users and user groups with this permission to directly access the KX II using an IP address when Local Access is enabled for the device in CC-SG. The device can be accessed from the Local Console, Remote Console, MPC, VKC, and AKC. When a device is accessed directly while it is under CC-SG management, access and connection activity is logged on the KX II. User authentication is performed based on KX II authentication settings. *Note: The Admin user group has this permission by default.*
Device Settings	Network settings, date/time settings, port configuration (channel names, power associations), event management (SNMP, Syslog), virtual media file server setups.
Diagnostics	Network interface status, network statistics, ping host, trace route to host, KX II diagnostics.
Maintenance	Backup and restore database, firmware upgrade, factory reset, reboot.
Modem Access	Permission to use the modem to connect to the KX II device.
PC-Share	Simultaneous access to the same target by multiple users. If you are using a tiered configuration in which a base KX II device is used to access multiple other tiered devices, all devices must share the same PC-Share setting. See ***Configuring and Enabling Tiering*** (on page 142) for more information on tiering.
Security	SSL certificate, security settings (VM Share, PC-Share), IP ACL.

Permission	Description
User Management	User and group management, remote. authentication (LDAP/LDAPS/RADIUS), login settings. If you are using a tiered configuration in which a base KX II device is used to access multiple other tiered devices, user, user group and remote authentication settings must be consistent across all devices. See ***Configuring and Enabling Tiering*** (on page 142) for more information on tiering.

Setting Port Permissions

For each server port, you can specify the access type the group has, as well as the type of port access to the virtual media and the power control. Please note that the default setting for all permissions is Deny.

Port access	
Option	**Description**
Deny	Denied access completely
View	View the video (but not interact with) the connected target server
Control	Control the connected target server. Control must be assigned to the group if VM and power control access will also be granted.

VM access	
Option	**Description**
Deny	Virtual media permission is denied altogether for the port
Read-Only	Virtual media access is limited to read access only
Read-Write	Complete access (read, write) to virtual media

Power control access	
Option	**Description**
Deny	Deny power control to the target server
Access	Full permission to power control on a target server

For blade chassis, the port access permission will control access to the URLs that have been configured for that blade chassis. The options are Deny or Control. In addition, each blade housed within the chassis has its own independent Port Permissions setting.

If you are using a tiered configuration in which a base KX II device is used to access multiple other tiered devices, the tiered device enforces individual port control levels. See ***Configuring and Enabling Tiering*** (on page 142) for more information on tiering.

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.

Note: See Alternate RADIUS Authentication Settings for information on additional settings if you are using Alternate RADIUS Authentication.

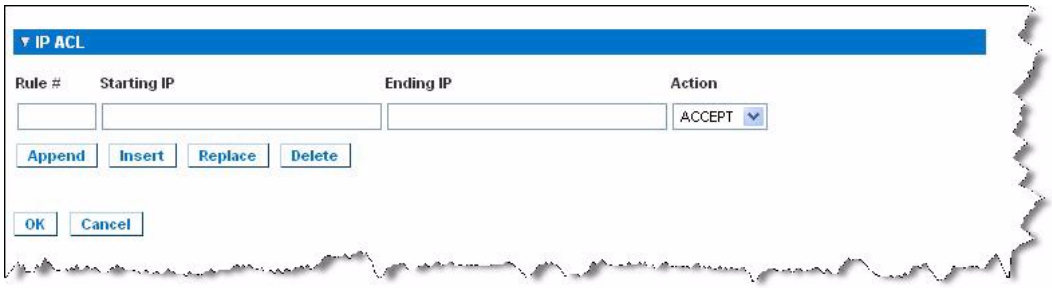
Group-Based IP ACL (Access Control List)

Important: Exercise caution when using group-based IP access control. It is possible to be locked out of your KX II if your IP address is within a range that has been denied access.

This feature limits access to the 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.

Important: The IP address 127.0.0.1 is used by the 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.



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 KX II device.
   - Drop - IP addresses set to Drop are denied access to the 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 number (#). A rule number 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 number you just typed equals an existing rule number, 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 number 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 number.

To delete a rule:

1. Specify the rule number 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.

```
Rule 1, Starting IP = 192.168.50.1, Ending IP = 192.168.55.255, Action = ACCEPT

Rule 2, Starting IP = 0.0.0.0, Ending IP = 255.255.255.255, Action = DROP
```

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

Note: Both IPv4 and IPv6 addresses are supported.

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. See Setting Permissions.
3. Set the Port Permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). See **Setting Port Permissions** (on page 115).
4. Set the IP ACL (optional). This feature limits access to the KX II device by specifying IP addresses. See **Group-Based IP ACL (Access Control List)** (on page 116).
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 KX II. This information is used to authenticate users attempting to access your KX II. Up to 254 users can be created for each user group.

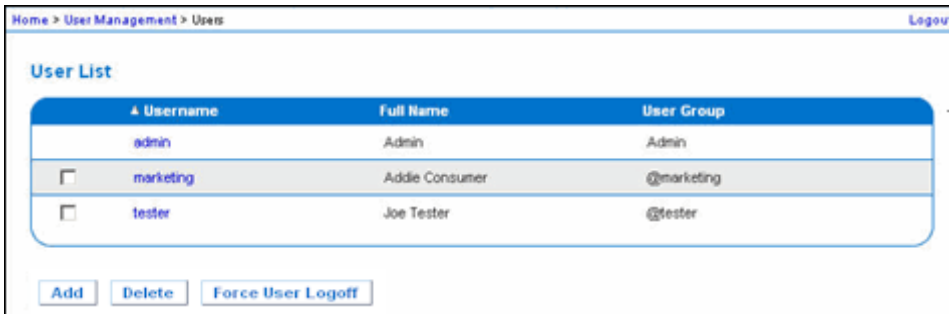
If you are using a tiered configuration in which a base KX II device is used to access multiple other tiered devices, users will need permission to access the base device and permissions to access each individual tiered device (as needed). When users log on to the base device, each tiered device is queried and the user can access each target server they have permissions to. See ***Configuring and Enabling Tiering*** (on page 142) for more information on tiering.

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.



Adding a New User

It is a good idea to define user groups before creating KX II users because, when you add a user, you must assign that user to an existing user group. See **Adding a New User Group** (on page 111).

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. See **Security Settings**.*

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>, which is the 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, see ***Setting Permissions for an Individual Group*** (on page 116).
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. Open the User List page by choosing User Management > User List.
2. Locate the user from among those listed on the User List page.
3. Click the user name. The User page opens.
4. On the User page, change the appropriate fields. See ***Adding a New User*** (on page 120) for information about how to get access the User page.

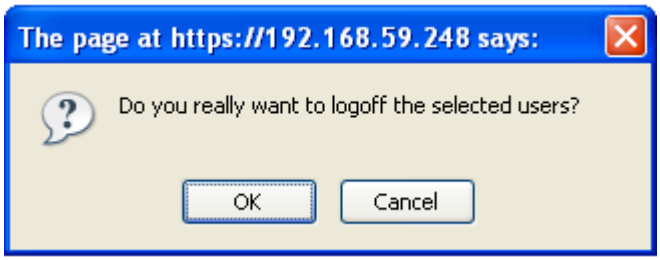
5. To delete a user, click Delete. You are prompted to confirm the deletion.
6. Click OK.

Logging a User Off (Force Logoff)

If you are an administrator, you are able to log off another locally authenticated user who is logged on to the KX II.

To log off a user:

1. Open the User List page by choosing User Management > User List or click the Connected User link in the left panel of the page.
2. Locate the user from among those listed on the User List page and select the checkbox next to their name.
3. Click the Force User Logoff button.
4. Click OK on the Logoff User dialog to forcefully log the user off.



5. A confirmation message is displayed to indicate that the user was logged off. This message contains the date and time the log off occurred. Click OK to close the message.

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

If you are using a tiered configuration in which a base KX II device is used to access multiple other tiered devices, the base device and the tiered devices must using the same authentication settings.

From the Authentication Settings page you can configure the type of authentication used for access to your KX II.

Note: When remote authentication (LDAP/LDAPS or RADIUS) is selected, if the user is not found, the local authentication database will also be checked.

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 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 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.

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:

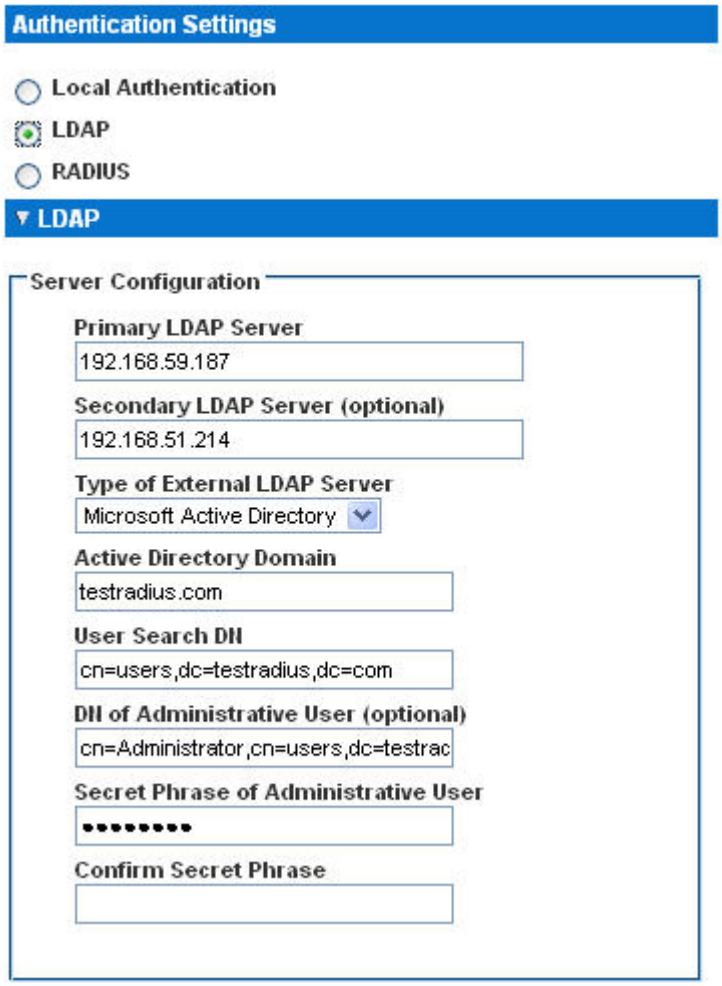
1. Click User Management > Authentication Settings to open the Authentication Settings page.
2. Select the LDAP radio button to enable the LDAP section of the page.
3. Click the LDAP icon to expand the LDAP section of the page.

Server Configuration

4. In the Primary LDAP Server field, type the IP address or DNS name of your LDAP/LDAPS remote authentication server (up to 256 characters). When the Enable Secure LDAP option is selected and the Enable LDAPS Server Certificate Validation option is selected, the DNS name must be used to match the CN of LDAP server certificate.
5. In the Secondary LDAP Server field, type the IP address or DNS name of your backup LDAP/LDAPS server (up to 256 characters). 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**
6. Type of External LDAP Server.
7. Select the 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.
8. Type the name of the Active Directory Domain if you selected Microsoft Active Directory. For example, *acme.com*. Consult your Active Directive Administrator for a specific domain name.

9. In the User Search DN field, enter the Distinguished Name of where in the LDAP database you want to begin searching for user information. Up to 64 characters can be used. An example base search value might be: `cn=Users,dc=raritan,dc=com`. Consult your authentication server administrator for the appropriate values to enter into these fields.
10. Enter the Distinguished Name of the Administrative User in the DN of Administrative User field (up to 64 characters). Complete this field if your LDAP server only allows administrators to search user information using the Administrative User role. 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`. **Optional**

11. If you entered a Distinguished Name for the Administrative User, you must enter the password that will be used to authenticate the Administrative User's DN against the remote authentication server. Enter the password in the Secret Phrase field and again in the Confirm Secret Phrase field (up to 128 characters).



LDAP/LDAP Secure

12. Select the Enable Secure LDAP checkbox if you would like to use SSL. This will enable the Enable LDAPS Server Certificate Validation checkbox. Secure Sockets Layer (SSL) is a cryptographic protocol that allows KX II to communicate securely with the LDAP/LDAPS server.
13. The default Port is 389. Either use the standard LDAP TCP port or specify another port.
14. The default Secure LDAP Port is 636. Either use the default port or specify another port. This field is only used when the Enable Secure LDAP checkbox is selected.

15. Select the Enable LDAPS Server Certificate Validation checkbox to use the previously uploaded root CA certificate file to validate the certificate provided by the server. If you do not want to use the previously uploaded root CA certificate file, leave this checkbox deselected. Disabling this function is the equivalent of accepting a certificate that has been signed by an unknown certifying authority. This checkbox is only available when the Enable Secure LDAP checkbox has been enabled.

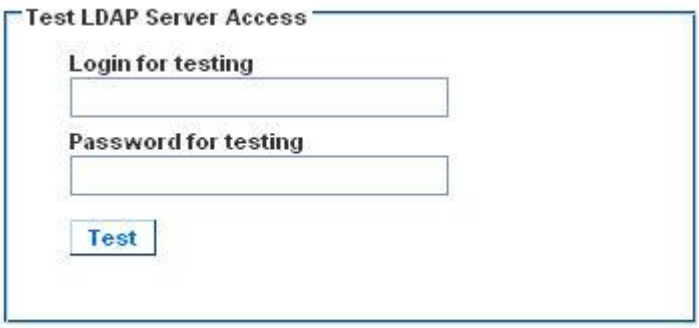
Note: When the Enable LDAPS Server Certificate Validation option is selected, in addition to using the Root CA certificate for validation, the server hostname must match the common name provided in the server certificate.

16. If needed, upload the Root CA Certificate File. This field is enabled when the Enable Secure LDAP option is selected. 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. If you are replacing a certificate for the LDAP/LDAPS server with a new certificate, you must reboot the KX II in order for the new certificate to take effect.

Test LDAP Server Access

17. The KX II provides you with the ability to test the LDAP configuration from the Authentication Settings page due to the complexity sometimes encountered with successfully configuring the LDAP server and KX II for remote authentication. To test the LDAP configuration, enter the login name and password in the "Login for testing" field and the "Password for testing" field respectively. This is the username and password you entered to access the KX II and that the LDAP server will use to authenticate you. Click Test.

Once the test is completed, a message will be displayed that lets you know the test was successful or, if the test failed, a detailed error message will be displayed. It will display successful result or detail error message in failure case. It also can display group information retrieved from remote LDAP server for the test user in case of success.



Returning User Group Information from Active Directory Server

The KX II supports user authentication to Active Directory® (AD) without requiring that users be defined locally on the 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 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, the KX II still supports this configuration and you do not need to perform the following operations. See Updating the LDAP Schema for information about updating the AD LDAP/LDAPS schema.

To enable your AD server on the KX II:

1. Using the 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 KX II users to the groups created in step 2.
4. From the KX II, enable and configure your AD server properly. See Implementing LDAP/LDAPS Remote Authentication.

Important Notes

- Group Name is case sensitive.
- The KX II provides the following default groups that cannot be 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 KX II group configuration, the 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.*
- Based on recommendations from Microsoft, Global Groups with user accounts should be used, not Domain Local Groups.

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. Click User Management > Authentication Settings to open the Authentication Settings page.
2. Click the RADIUS radio button to enable the RADIUS section of the page.
3. Click the 

icon to expand the RADIUS section of the page.
4. In the Primary Radius Server and Secondary Radius Server fields, type the IP address of your primary and optional secondary remote authentication servers, respectively (up to 256 characters).
5. In the Shared Secret fields, type the server secret used for authentication (up to 128 characters).

   The shared secret is a character string that must be known by both the KX II and the RADIUS server to allow them to communicate securely. It is essentially a password.
6. The Authentication Port default is port is 1812 but can be changed as required.
7. The Accounting Port default port is 1813 but can be changed as required.
8. The Timeout is recorded in seconds and default timeout is 1 second, but can be changed as required.

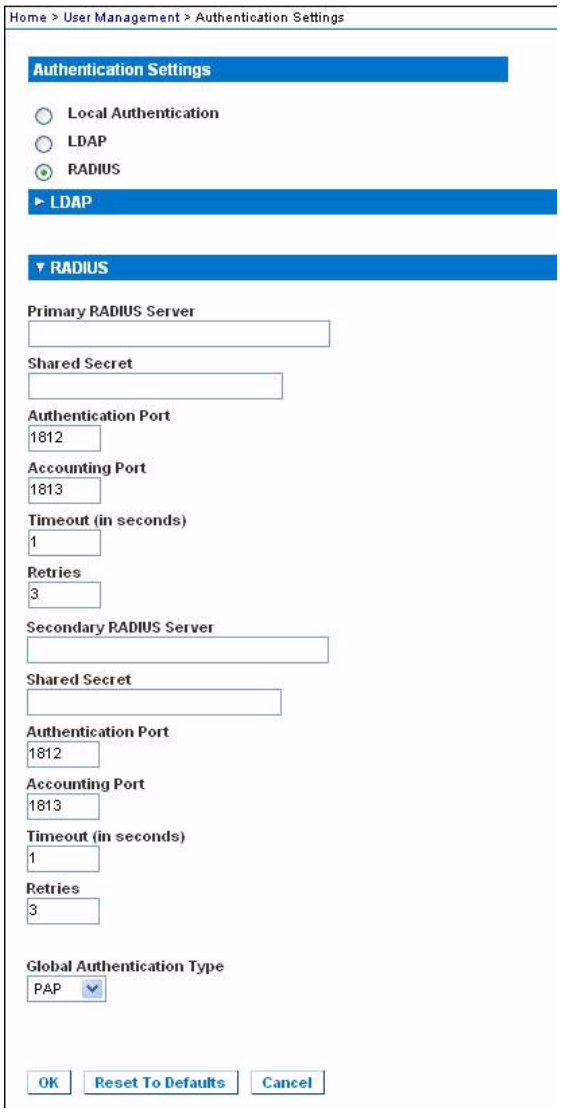
   The timeout is the length of time the KX II waits for a response from the RADIUS server before sending another authentication request.

9. The default number of retries is 3 Retries.

   This is the number of times the KX II will send an authentication request to the RADIUS server.

10. Choose the Global Authentication Type 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.



Note: Both IPv4 and IPv6 addresses are supported.

Cisco ACS 5.x for RADIUS Authentication

If you are using a Cisco ACS 5.x server, after you have configured the KX II for RADIUS authentication, complete the following steps on the Cisco ACS 5.x server.

Note: The following steps include the Cisco menus and menu items used to access each page. Please refer to your Cisco documentation for the most up to date information on each step and more details on performing them.

- Add the KX II as a AAA Client (**Required**) - Network Resources > Network Device Group > Network Device and AAA Clients
- Add/edit users (**Required**) - Network Resources > Users and Identity Stores > Internal Identity Stores > Users
- Configure Default Network access to enable CHAP Protocol (**Optional**) - Policies > Access Services > Default Network Access
- Create authorization policy rules to control access (**Required**) - Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
  - Dictionary Type: RADIUS-IETF
  - RADIUS Attribute: Filter-ID
  - Attribute Type: String
  - Attribute Value: Raritan:G{KVM_Admin} (where KVM_Admin is group name created locally on Dominion KVM Switch). Case sensitive.
- Configure Session Conditions (Date and Time) (**Required**) - Policy Elements > Session Conditions > Date and Time
- Configure/create the Network Access Authorization Policy (**Required**) - Access Policies > Access Services > Default Network Access>Authorization

Returning User Group Information via RADIUS

When a RADIUS authentication attempt succeeds, the KX II 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 KX II modem will use to dial back to the user account.

RADIUS Communication Exchange Specifications

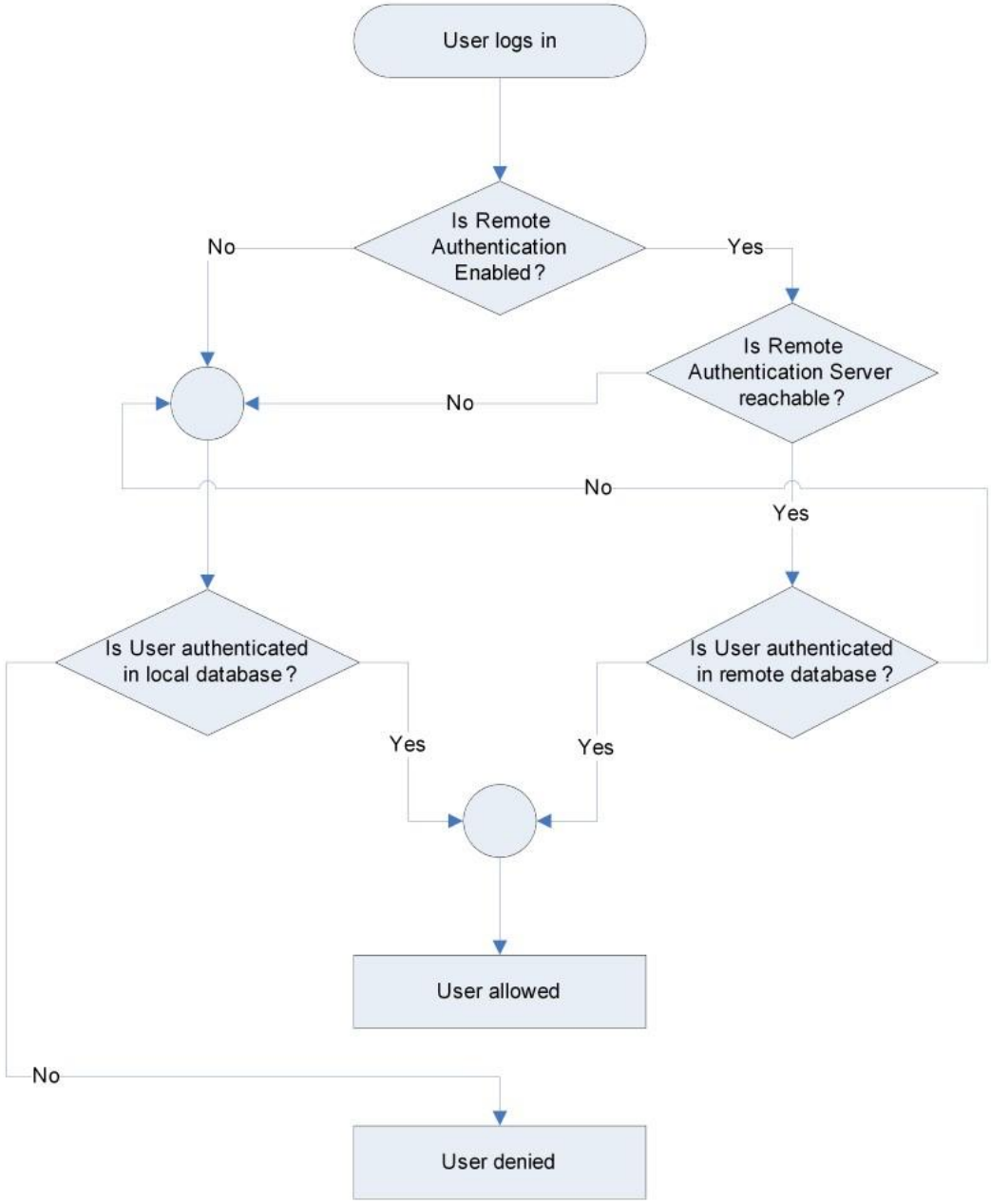
The KX II sends the following RADIUS attributes to your RADIUS server:

Attribute	Data
Log in	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-IP-Address (4)	The IP address for the 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.
NAS-IP-Address (4)	The IP address for the KX II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
Log out	
Accounting-Request(4)	

Attribute	Data
Acct-Status (40)	Stop(2) - Stops the accounting
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP address for the KX II.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

User Authentication Process

Remote authentication follows the process specified in the flowchart below:

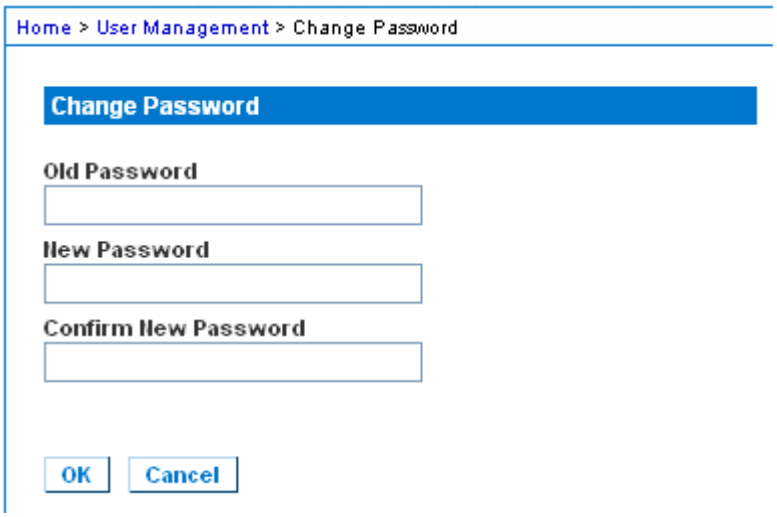


Changing a Password

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, see **Strong Passwords** *(on page 198).*



Chapter 8 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 KX II.

There are two options available to set up your IP configuration:

- None (default) - This is the recommended option (static IP). Since the 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. See Network Basic Settings.
3. Update the LAN Interface Settings. See LAN Interface Settings.
4. Click OK to set these configurations. If your changes require rebooting the device, a reboot message appears.

To reset to factory defaults:

- Click Reset to Defaults.

Note: Both IPv4 and IPv6 addresses are supported.

Network Basic Settings

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, see **Network Settings**.

To assign an IP address:

1. Choose Device Settings > Network. The Network Settings page opens.
2. Specify a meaningful Device Name for your KX II device. Up to 32 alphanumeric characters using valid special characters and no spaces.
3. In the IPv4 section, enter or select the appropriate IPv4-specific network settings:
   a. Enter the IP Address if needed. The default IP address is 192.168.0.192.
   b. Enter the Subnet Mask. The default subnet mask is 255.255.255.0.
   c. Enter the Default Gateway if None is selected from the IP Auto Configuration drop-down.
   d. Enter the Preferred DHCP Host Name if DHCP is selected from the IP Auto Configuration drop-down.
   e. Select the IP Auto Configuration. The following options are available:
   - None (Static IP) - This option requires that you manually specify the network parameters.

     This is the recommended option because the KX II is an infrastructure device and its IP address should not change.
   - DHCP - Dynamic Host Configuration Protocol is used by networked computers (clients) to obtain unique IP addresses and other parameters from a DHCP server.

     With this option, network parameters are assigned by the DHCP server. If DHCP is used, enter the Preferred host name (DHCP only). Up to 63 characters.
4. If IPv6 is to be used, enter or select the appropriate IPv6-specific network settings in the IPv6 section:
   a. Select the IPv6 checkbox to activate the fields in the section.
   b. Enter a Global/Unique IP Address. This is the IP address assigned to the KX II.
   c. Enter the Prefix Length. This is the number of bits used in the IPv6 address.

d. Enter the Gateway IP Address.

e. Link-Local IP Address. This address is automatically assigned to the device. It is used for neighbor discovery or when no routers are present. **Read-Only**

f. Zone ID. This identifies the device with which the address is associated. **Read-Only**

g. Select the IP Auto Configuration. The following options are available:

- 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: Global/Unique IP Address, Prefix Length, and Gateway IP Address allowing you to manually set the IP configuration.

- Router Discovery - Use this option to automatically assign IPv6 addresses that have Global or Unique Local significance beyond that of the Link Local, which only applies to a directly connected subnet.

5. Select Obtain DNS Server Address Automatically if DHCP is selected and Obtain DNS Server Address is enabled. When Obtain DNS Server Address Automatically, the DNS information provided by the DHCP server will be used.

6. If Use the Following DNS Server Addresses is selected, regardless of whether DHCP is selected or not, the addresses entered in this section will be used to connect to the DNS server.

   Enter the following information if the Following DNS Server Addresses option is selected. These addresses are the primary and secondary DNS addresses that will be used if the primary DNS server connection is lost due to an outage.

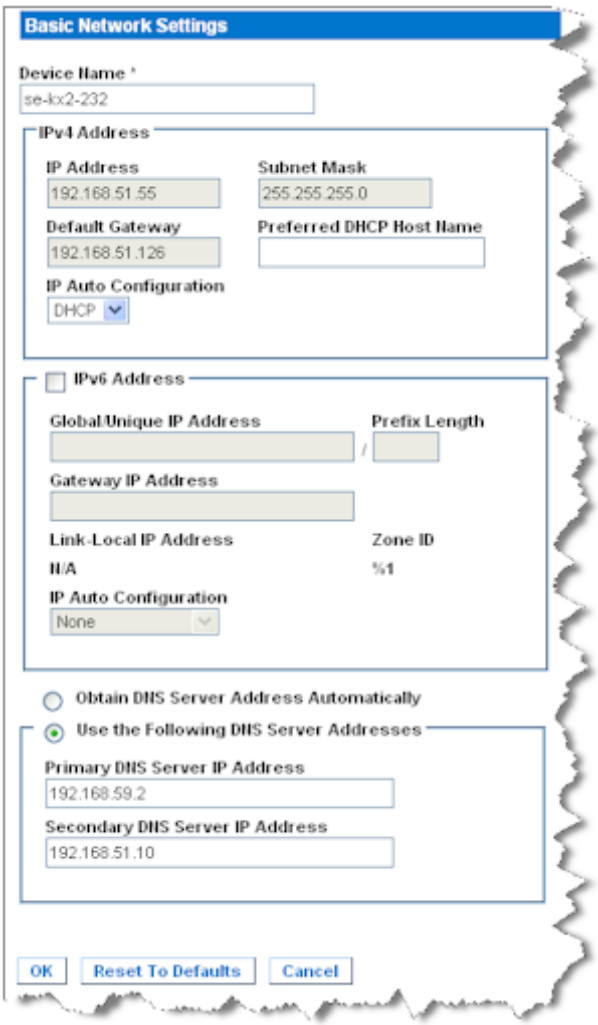
   a. Primary DNS Server IP Address

   b. Secondary DNS Server IP Address

7. When finished, click OK.

See ***LAN Interface Settings*** (on page 138) for information in configuring this section of the Network Settings page.

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 KX II LAN Interface Speed & Duplex field to 100 Mbps/Full Duplex (or whatever option is appropriate to your network) addresses the issue. See the **Network Settings** *(on page 135) page for more information.*



LAN Interface Settings

1. The current parameter settings are identified in the Current LAN interface parameters field.
2. Choose the LAN Interface Speed & Duplex from the following options:

- 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.

See ***Network Speed Settings*** (on page 280) for more information.

3. Select the Enable Automatic Failover checkbox to allow the 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 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 KX II checks the status of the network path to the designated gateway. The default ping interval is 30 seconds.
- Timeout (seconds) - Timeout determines how long a designated gateway remains unreachable via the network connection before a fail over occurs.

Note: The ping interval and timeout can be configured to best meet the local network conditions. The timeout should be set to allow for at least two or more ping requests to be transmitted and responses returned. For example, if a high rate of failover is observed due to high network utilization, the timeout should be extended to 3 or 4 times the ping interval.

4. Select the Bandwidth.
5. Click OK to apply the LAN settings.

Device Services

The Device Services page allows you to configure the following functions:

- Enable SSH access.
- Enable tiering for the base KX II.
- Enter the discovery port.
- Enable direct port access.
- Enable the AKC Download Server Certificate Validation feature if you are using AKC.

Enabling SSH

Enable SSH access to allow administrators to access the KX II via the SSH v2 application.

To enable SSH access:

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Select Enable SSH Access.
3. Enter the SSH Port information. The standard SSH TCP port number is 22 but the port number can be changed to provide a higher level of security operations.
4. Click OK.

HTTP and HTTPS Port Settings

You are able to configure HTTP and/or HTTPS ports used by the KX II. For example, if you are using the default HTTP port 80 for another purpose, changing the port will ensure the device does not attempt to use it.

To change the HTTP and/or HTTPS port settings:

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Enter the new ports in the HTTP Port and/or HTTPS Port fields.
3. Click OK.

Entering the Discovery Port

The 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 except 80 and 443. To access the KX II from beyond a firewall, your firewall settings must enable two-way communication through the default Port 5000 or a non-default port configured here.

To enable the discovery port:

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Enter the Discovery Port.
3. Click OK.

Configuring and Enabling Tiering

The tiering feature allows you to access KX II targets and PDUs through one base KX II device. This feature is available for standard KX II devices as well as KX2-832 and KX2-864 devices. Devices can be added and removed from a configuration as needed up to a maximum of two tiered levels.

When setting up the devices, you will use specific CIMS for specific configurations. See ***Tiering - Target Types, Supported CIMS and Tiering Configurations*** (on page 144) for a description of the targets that can be included in a tiered configuration, CIM compatibility and device configuration information.

Before adding tiered devices, you must enable tiering for the base device and the tiered devices. Enable base devices on the Device Settings page. Enable tiered devices on the Local Port Settings page. Once devices are enabled and configured, they appear on the Port Access page (***Port Access Page*** (on page 43)).

When a KX II is configured to function as a base device or tiered device, they will be displayed as:

- Configured As Base Device in the Device Information section of the left panel of the KX II interface for base devices.
- Configured As Tier Device in the Device Information section of the left panel of the KX II interface for tiered devices.
- The base device will be identified as Base in the left panel of the tiered device's interface under Connect User.
- Target connections to a tier port from the base will be displayed as 2 ports connected.

The base device provides remote and local access over a consolidated port list from the Port Access page. Tiered devices provide remote access from their own port lists. Local access is not available on the tiered devices when Tiering is enabled.

Tiering also supports the use of KVM switches to switch between servers. See ***Configuring KVM Switches*** (on page 160).

Enabling Tiering

Connect from a target server port on the base device to the tier KX II Local Access port video/keyboard/mouse ports using a D2CIM-DVUSB.

If the tier device is a KX2-832 or KX2-864, connect from a target server port on the base device directly to the tier KX2-832/KX2-864 Extended Local port.

To enable tiering:

1. From the tier base, choose Device Settings > Device Services. The Device Service Settings page appears.
2. Select Enable Tiering as Base.
3. In the Base Secret field, enter the secret shared between the base and the tiered devices. This secret is required for the tiered devices to authenticate the base device. You will enter the same secret word for the tiered device.
4. Click OK.
5. Enable the tiered devices. From the tiered device, choose Device Settings > Local Port Settings.
6. In the Enable Local Ports section of the page, select Enable Local Port Device Tiering.
7. In the Tier Secret field, enter the same secret word you entered for the base device on the Device Settings page.
8. Click OK.

Tiering - Target Types, Supported CIMS and Tiering Configurations

Blade Chassis

Blade chassis that attached directly to the base are accessible.

Power Control

You can power on and off targets that are a part of the tiered configuration. These targets are accessed from the Port Access page.

KX II PDU outlets can be accessed and controlled via a tiered configuration with either the KX II or KXII-832 and KXII-864 models. If targets and outlets are associated, power control is available from the Port Access page. Targets and PDU outlet associations are limited to those attached to the same KX II.

PDUs attached to the base or tiered KX IIs are displayed on the Power page drop-down along with the statistics for the selected powerstrip.

Outlet level control is available as well. Specifically, you can power off and power on outlets that are currently on, but you cannot power cycle outlets that are currently off.

KX II to KX II or KXII-8xx Local Port Configuration - Compatible CIMS

The following CIMS are compatible when you are configuring a base KX II to access and control either additional KX II or KXII-832 and KXII-864 models, as well as KX II PDUs and blade chassis.

If you are using a KX II to KX II configuration, the D2CIM-DVUSB must be used. If you are using a KX II to KXII-8xx configuration, only the extended local port can be used.

If you are using a configuration that consists of a KX II and KXII-832 or KXII-864, each device must be running the same firmware. Where blade chassis are a part of a configuration, each blade chassis counts as one target port.

Unsupported and Limited Features on Tiered Targets

The following features are not supported on tiered targets:

- Blade chassis on tiered devices
- Smartcards on tiered devices
- Virtual media tiered devices
- MCCAT as a tiered device

Port group management is limited to creating port groups of members directly attached to the base.

Cabling Example in Tiered Configurations

The following diagram illustrates the cabling configurations between a KX II tiered device and a KX II base device. Connect from a target server port on the base device to the tier KX II Local Access port video/keyboard/mouse ports using a D2CIM-DVUSB.

If the tier device is a KX2-832 or KX2-864, connect from a target server port on the base device directly to the tier KX2-832/KX2-864 Extended Local port.

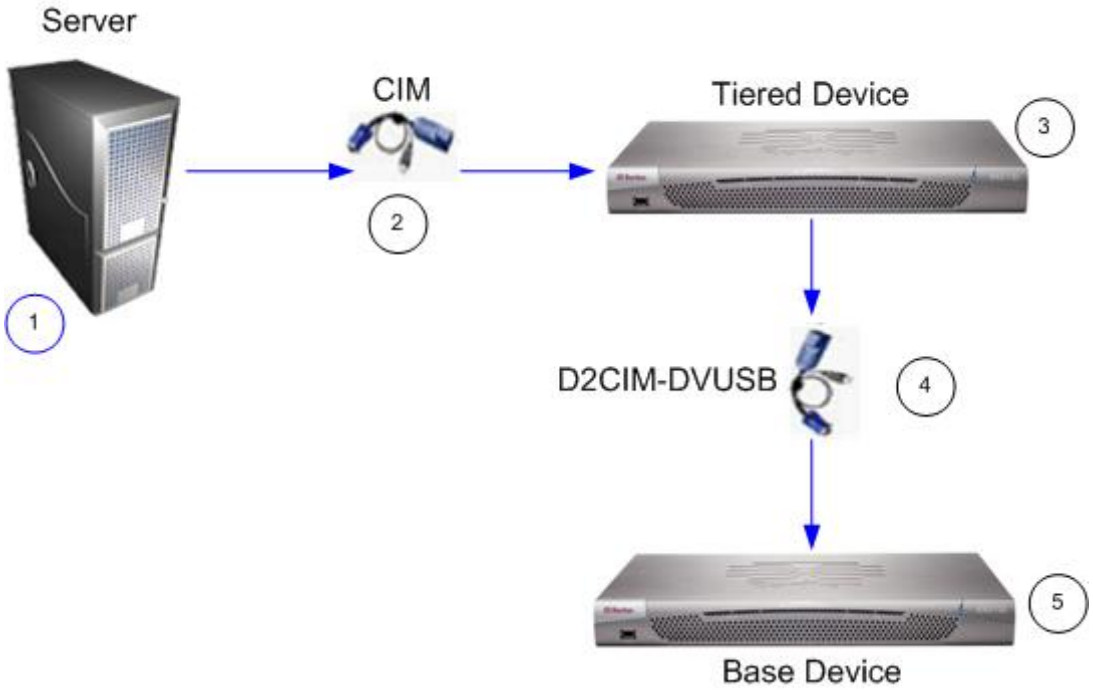


Diagram key	
1	Target server
2	CIM from target server to the KX II tiered device
3	KX II tiered device
4	D2CIM-DVUSB CIM from the KX II tiered device to the KX II base device
5	KX II base device

Enabling Direct Port Access via URL

Direct port access allows users to bypass having to use the device's Login dialog and Port Access page. This feature also provides the ability to enter a username and password directly and proceed to the target if the username and password is not contained in the URL.

The following is important URL information regarding direct port access:

If you are using VKC and direct port access:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number

If you are using AKC and direct port access:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number&client=akc

Where:

- Username and password are optional. If they are not provided, a login dialog will be displayed and, after being authenticated, the user will be directly connected to the target.
- The port may be a port number or port name. If you are using a port name, the name must be unique or an error is reported. If the port is omitted altogether, an error is reported.
- For blade chassis, the port is designated <port number>'-'<slot number>. For example, 1-2 for blade chassis connected to port 1, slot 2.
- Client=akc is optional unless you are using the AKC client. If client=akc is not included, VKC is used as the client.

To enable direct port access:

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Select Enable Direct Port Access via URL if you would like users to have direct access to a target via the Dominion device by passing in the necessary parameters in the URL.
3. Click OK.

Enabling the AKC Download Server Certificate Validation

If you are using the AKC client, you can choose to use the Enable AKC Download Server Certificate Validation feature or opt not to use this feature.

Option 1: Do Not Enable AKC Download Server Certificate Validation (default setting)

If you do not enable AKC Download Server Certificate Validation, all Dominion device users and CC-SG Bookmark and Access Client users must:

- Ensure the cookies from the IP address of the device that is being accessed are not currently being blocked.
- Windows Vista, Windows 7 and Windows 2008 server users should ensure that the IP address of the device being accessed is included in their browser's Trusted Sites Zone and that Protected Mode is not on when accessing the device.

Option 2: Enable AKC Download Server Certificate Validation

If you do enable AKC Download Server Certificate Validation:

- Administrators must upload a valid certificate to the device or generate a self-signed certificate on the device. The certificate must have a valid host designation.
- Each user must add the CA certificate (or a copy of self-signed certificate) to the Trusted Root CA store in their browser.

To install the self-signed certificate when using Windows Vista® operating system and Windows 7® operating system:

1. Include the KX II IP address in the Trusted Site zone and ensure 'Protected Mode' is off.
2. Launch Internet Explorer® using the KX II IP address as the URL. A Certificate Error message will be displayed.
3. Select View Certificates.
4. On the General tab, click Install Certificate. The certificate is then installed in the Trusted Root Certification Authorities store.
5. After the certificate is installed, the KX II IP address can be removed from the Trusted Site zone.

To enable AKC download server certificate validation:

1. Choose Device Settings > Device Services. The Device Service Settings page opens.
2. Select the Enable AKC Download Server Certificate Validation checkbox or you can leave the feature disabled (default).
3. Click OK.

Configuring Modem Settings

To configure modem settings:

1. Click Device Settings > Modem Settings to open the Modem Settings page.
2. Select the Enable Modem checkbox. This will enable the Serial Line Speed and Modem Init String field.
3. The Serial Line Speed of the modem is set to 115200. **Read-only**
4. Enter the initial modem string in the Modem Init String field. If the modem string is left blank, the following string is sent to the modem by default: ATZ OK AT OK.

   This information is used to configure modem settings. Because different modems have different ways of settings these values, this document does not specify how to set these values, rather the user should refer to the modem to create the appropriate modem-specific string.

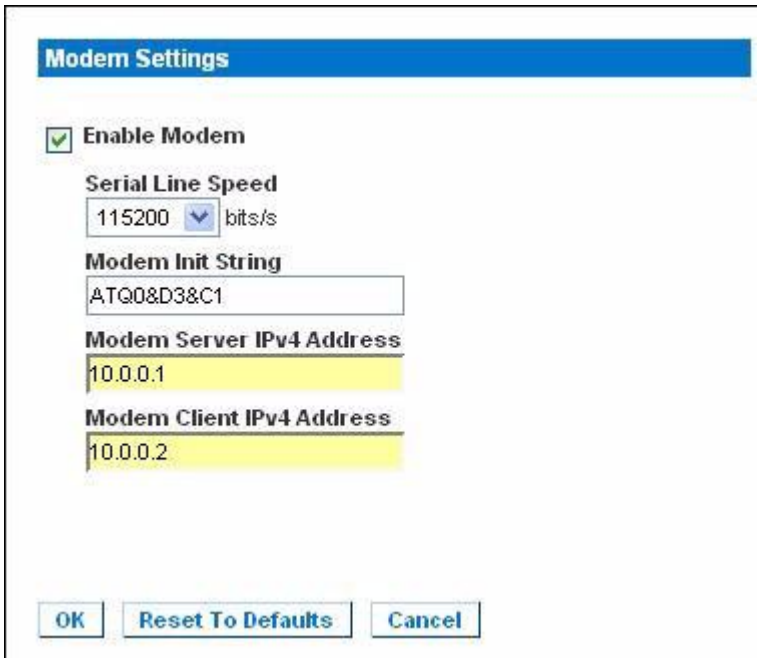
   a. Modem Settings:

      - Enable RTS/CTS flow control
      - Send data to the computer on receipt of RTS
      - CTS should be configured to only drop if required by flow control.
      - DTR should be configured for Modem resets with DTR toggle.
      - DSR should be configured as always on.
      - DCD should be configured as enabled after a carrier signal is detected. (that is, DCD should only be enabled when modem connection is established with the remote side)

5. Enter the IPv4 modem server address in the Modem Server IPv4 Address field and the client modem address in the Modem Client IPv4 Address field.

Note: The modem client and server IP addresses must be on the same subnet and cannot overlap the KX LAN subnet.

6. Click OK to commit your changes or click Reset to Defaults to return the settings to their defaults.



See ***Certified Modems*** (on page 271) for information on certified modems that work with the KX II. For information on settings that will give you the best performance when connecting to the KX II via modem, see Creating, Modifying and Deleting Profiles in MPC - Generation 2 Devices in the **KVM and Serial Access Clients Guide**.

Note: Modem access directly to the KX II HTML interface is not supported. You must use standalone MPC to access the KX II via modem.

Configuring Date/Time Settings

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

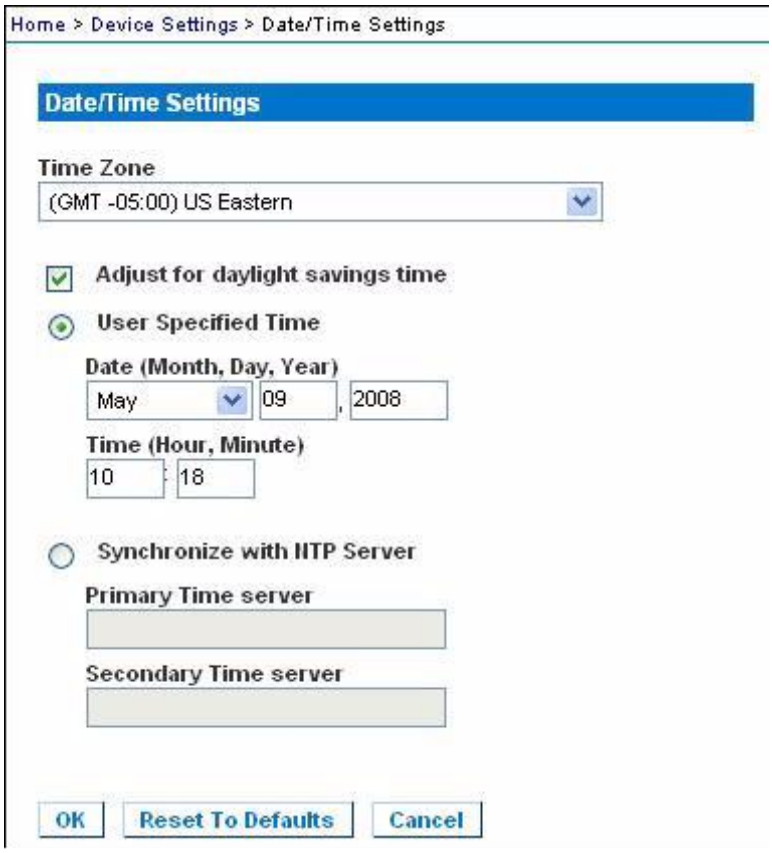
- Manually set the date and time.
- Synchronize the date and time with a Network Time Protocol (NTP) server.

To set the date and time:

1. Choose Device Settings > Date/Time. The Date/Time Settings page opens.
2. Choose your time zone from the Time Zone drop-down list.

3. To adjust for daylight savings time, check the "Adjust for daylight savings time" checkbox.
4. 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.

     For the User Specified Time option, enter the date and time. For the time, use the hh:mm format (using a 24-hour clock).
   - Synchronize with NTP Server - Choose this option to synchronize the date and time with the Network Time Protocol (NTP) Server.
5. 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**
6. Click OK.



Note: Both IPv4 and IPv6 addresses are supported.

Event Management

The KX II Event Management feature allows you enable and disable the distribution of system events to SNMP Managers, the 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.

Configuring 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. The 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.
2. Select SNMP Logging Enabled. 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 KX II Console interface, a contact name related to this device, and where the Dominion device is physically located.
4. Type the Agent Community String (the device's string). An SNMP community is the group to which devices and management stations running SNMP belong. 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/Hostname, 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.

To configure the Syslog (enable Syslog forwarding):

1. Select Enable Syslog Forwarding to log the device's messages to a remote Syslog server.
2. Type the IP Address/Hostname of your Syslog server in the IP Address field.

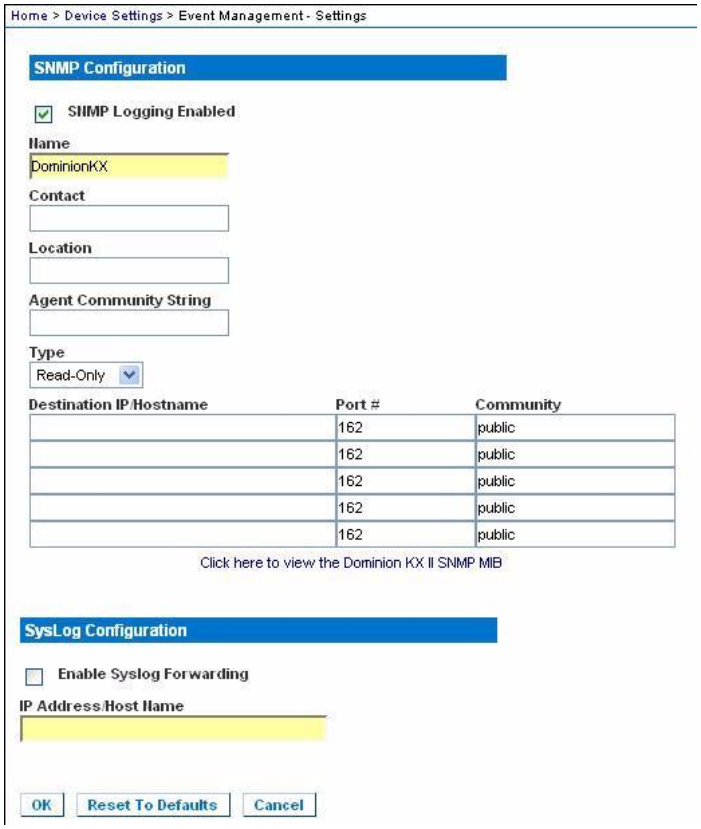
3. Click OK.

To reset to factory defaults:

- Click Reset To Defaults.

Note: Both IPv4 and IPv6 addresses are supported.

Note: IPv6 addresses cannot exceed 80 characters in length for the host name.



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

To select events and their destinations:

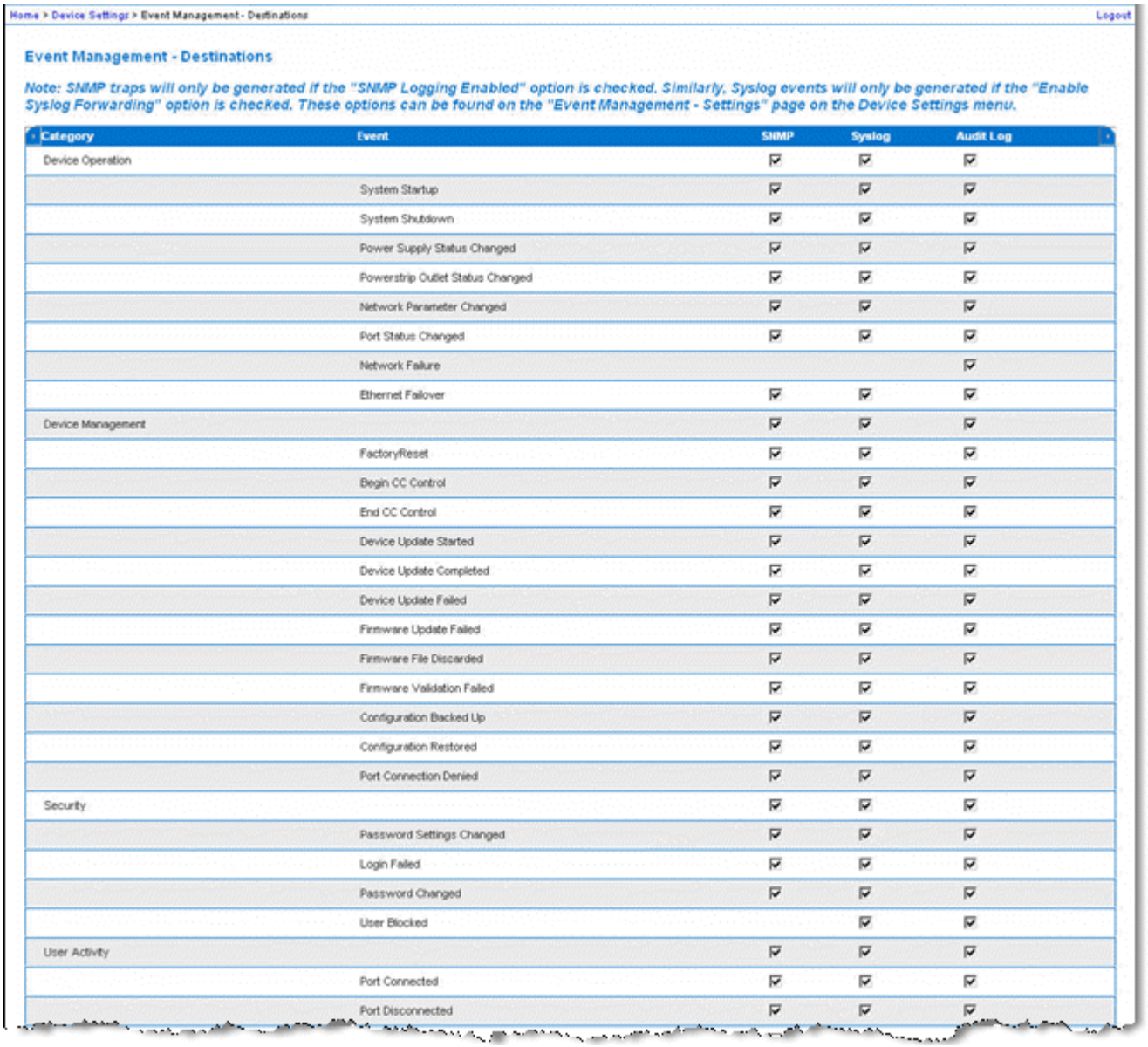
1. Choose Device Settings > Event Management - Destinations. The Event Management - Destinations page opens.

   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 Reset To Defaults.

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

SNMP Agent Configuration

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

SNMP Trap Configuration

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

Trap Name	Description
bladeChassisCommError	A communications error with blade chassis device connected to this port was detected. *Note: Not supported by the KX II-101.*
configBackup	The device configuration has been backed up.
configRestore	The device configuration has been restored.
deviceUpdateFailed	Device update has failed.
deviceUpgradeCompleted	The KX II has completed update via an RFP file.
deviceUpgradeStarted	The 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.
groupAdded	A group has been added to the 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

Trap Name	Description
	communicate over the network.
networkParameterChanged	A change has been made to the network parameters.
passwordSettingsChanged	Strong password settings have changed.
portConnect	A previously authenticated user has begun a KVM session.
portConnectionDenied	A connection to the target port was denied.
portDisconnect	A user engaging in a KVM session closes the session properly.
portStatusChange	The port has become unavailable.
powerNotification	The power outlet status notification: 1=Active, 0=Inactive.
powerOutletNotification	Power strip device outlet status notification.
rebootCompleted	The KX II has completed its reboot.
rebootStarted	The 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.
userConnectionLost	A user with an active session has experienced an abnormal session termination.
userDeleted	A user account has been deleted.
userForcedLogout	A user was forcibly logged out by Admin
userLogin	A user has successfully logged into the KX II and has been authenticated.
userLogout	A user has successfully logged out of the 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.

Trap Name	Description
userSessionTimeout	A user with an active session has experienced a session termination due to timeout.
userUploadedCertificate	A user uploaded a SSL certificate.
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

The 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 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.

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 PowerIn1 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 PowerIn2 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 KX II does NOT report power supply status to CommandCenter. Dominion I (generation 1), however, does report power supply status to CommandCenter.

Configuring Ports

The Port Configuration page displays a list of the KX II ports. Ports connected to KVM target servers (blades and standard servers) and rack PDUs (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 KX II physical port.

To access a port configuration:

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

   This page is initially displayed in port number order, but can be sorted on any of the fields by clicking on the column heading.

   - Port Number - Numbered from 1 to the total number of ports available for the KX II 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

Port type	Description
DCIM	Dominion CIM
Not Available	No CIM connected
PCIM	Paragon CIM

Port type	Description
PowerStrip (rack PDU)	Power strip connected
VM	Virtual media CIM (D2CIM-VUSB and D2CIM-DVUSB)
Blade Chassis	Blade chassis and the blades associated with that chassis (displayed in a hierarchical order)

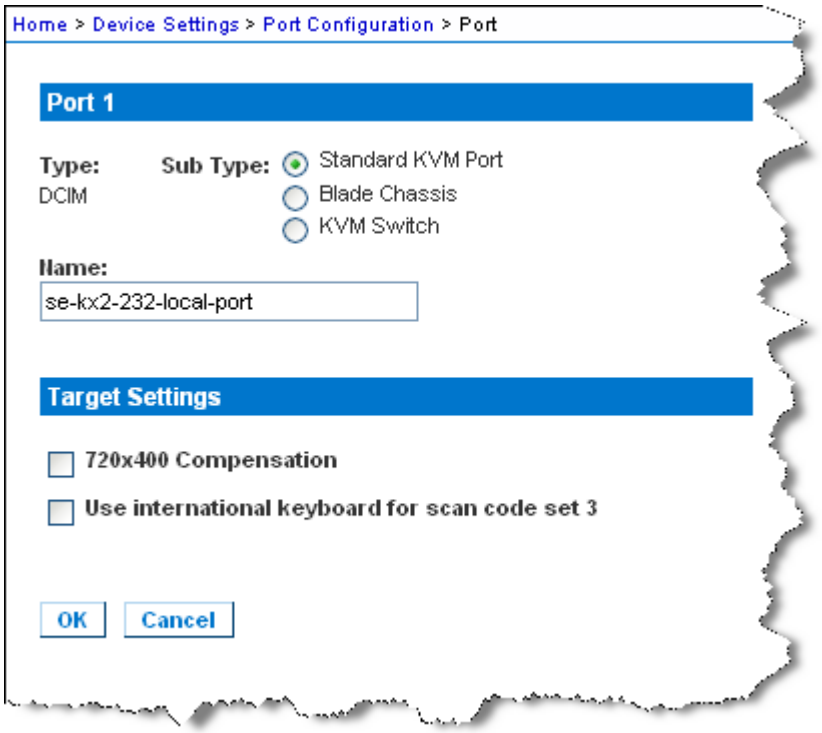
2. Click the Port Name for the port you want to edit.
   - For KVM ports, the Port page for KVM and blade chassis ports is opened.
   - For rack PDUs, the Port page for rack PDUs (power strips) is opened. From this page, you can name the rack PDUs and their outlets.

Configuring Standard Target Servers

To name the target servers:

1. Connect all of the target servers if you have not already done so. See Step 3: Connect the Equipment for a description of connecting the equipment.
2. Choose Device Settings > Port Configuration. The Port Configuration page opens.
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. Select Standard KVM Port as the subtype for the port.
6. In the Target Settings section, select 720x400 Compensation if you are experiencing display issues when the target is using this resolution.
7. Select 'Use international keyboard for scan code set 3' if connecting to the target with a DCIM-PS2 and require the use of scan code set 3 with an international keyboard.

8. Click OK.



Configuring KVM Switches

The KX II also supports use of hot key sequences to switch between targets. In addition to using hot key sequences with standard servers, KVM switching is supported by blade chassis and in tiered configurations.

Important: In order for user groups to see the KVM switch that you create, you must first create the switch and then create the group. If an existing user group needs to see the KVM switch you are creating, you must recreate the user group.

To configure KVM switches:

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.
2. Click the Port Name of the target server you want to rename. The Port Page opens.
3. Select KVM Switch.
4. Select the KVM Switch Model.

Note: Only one switch will appear in the drop-down.

5. Select KVM Switch Hot Key Sequence.
6. Enter the Maximum Number of Target Ports (2-32).
7. In the KVM Switch Name field, enter the name you want to use to refer to this port connection.
8. Activate the targets that the KVM switch hot key sequence will be applied to. Indicate the KVM switch ports have targets attached by selecting 'Active' for each of the ports.
9. In the KVM Managed Links section of the page, you are able to configure the connection to a web browser interface if one is available.
   a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.
   b. URL Name - Enter the URL to the interface.
   c. Username - Enter the username used to access the interface.
   d. Password - Enter the password used to access the interface.
   e. Username Field - Enter the username parameter that will be used in the URL. For example *username*=admin, where *username* is the username field.
   f. Password Field - Enter the password parameter that will be used in the URL. For example *password*=raritan, where *password* is the password field.
10. Click OK.

To change the active status of a KVM switch port or URL:

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.
2. Click the Port Name of the target server you want to rename. The Port Page opens.
3. Deselect the Active checkbox next to the KVM switch target port or URL to change its active status.
4. Click OK.

Configuring Rack PDU (Power Strip) Targets

The KX II allows you to connect rack PDUs (power strips) to KX II ports. KX II rack PDU configuration is done from the KX II Port Configuration page.

Connecting a Rack PDU

Raritan PX series rack PDUs (power strips) are connected to the KX II using the D2CIM-PWR CIM.

To connect the rack PDU:

1. Connect the male RJ-45 of the D2CIM-PWR to the female RJ-45 connector on the serial port of the rack PDU.
2. Connect the female RJ-45 connector of the D2CIM-PWR to any of the available female system port connectors on the KX II using a straight through Cat5 cable.
3. Attach an AC power cord to the target server and an available rack PDU outlet.
4. Connect the rack PDU to an AC power source.
5. Power on the device.

Naming the Rack PDU in the KX II (Port Page for Power Strips)

Note: PX rack PDUs (power strips) can be named in the PX as well as in KX II.

The Port page opens when you select a port from the Port Configuration page that is connected to a Raritan remote rack PDU. The Type and the Name fields are prepopulated.

Note: The (CIM) Type cannot be changed.

The following information is displayed for each outlet on the rack PDU: [Outlet] Number, Name, and Port Association.

Use this page to name the rack PDU and its outlets. All names can be up to 32 alphanumeric characters and can include special characters.

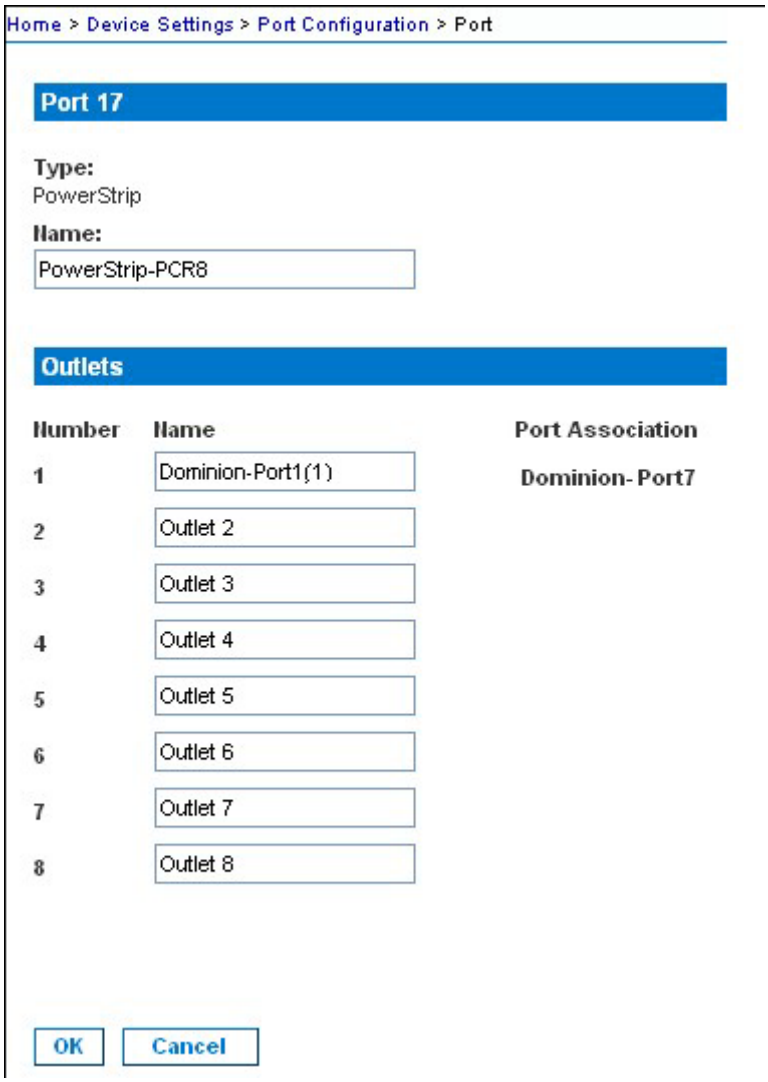
Note: When a rack PDU is associated with a target server (port), the outlet name is replaced by the target server name (even if you assigned another name to the outlet).

To name the rack PDU (and outlets):

Note: CommandCenter Service Gateway does not recognize rack PDU names containing spaces.

1. Enter the Name of the rack PDU (if needed).
2. Change the [Outlet] Name if desired. (Outlet names default to the outlet #.)

3. Click OK.



Associating Outlets with Target Servers on KX II

The Port page opens when you click on a port on the Port Configuration page. 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 rack PDU (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 rack PDU(s)
- Power CIMs (D2CIM-PWR)

To make power associations (associate rack PDU outlets to KVM target servers):

Note: When a rack PDU 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 rack PDU from the Power Strip Name drop-down list.
2. For that rack PDU, 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.

Removing Power Associations

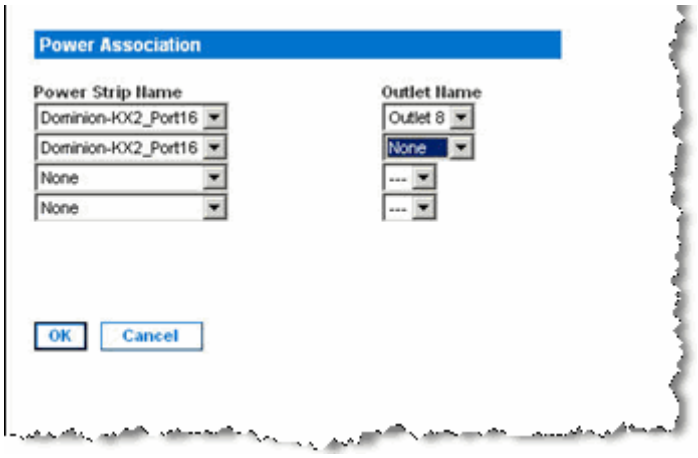
When disconnecting target servers and/or rack PDUs from KXII, all power associations should first be deleted. When a target has been associated with a rack PDU and the target is removed from the KX II, the power association remains. When this occurs, you are not able to access the Port Configuration for that disconnected target server in Device Settings so that the power association can be properly remove.

To remove a rack PDU association:

1. Select the appropriate rack PDU from the Power Strip Name drop-down list.
2. For that rack PDU, 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 rack PDU/outlet association is removed and a confirmation message is displayed.

To remove a rack PDU association if the rack PDU has been removed from the target:

1. Click Device Settings > Port Configuration and then click on the active target.
2. Associate the active target to the disconnected power port. This will break the disconnected target's power association.
3. Finally, associate the active target to the correct power port.



Configuring Blade Chassis

In addition to standard servers and rack PDUs (power strips), you can control blade chassis that are plugged into a Dominion device port. Up to eight blade chassis can be managed at a given time.

As with standard servers, blade chassis are autodetected once they are connected. When a blade server chassis is detected, a default name is assigned to it and it is displayed on the Port Access page along with standard target servers and rack PDUs (see ***Port Access Page*** (on page 43)). The blade chassis is displayed in an expandable, hierarchical list on the Port Access page, with the blade chassis at the root of the hierarchy and the individual blades labeled and displayed below the root. Use the Expand Arrow icon next to the root chassis to display the individual blades.

Note: To view the blade chassis in a hierarchal order, blade-chassis subtypes must be configured for the blade server chassis.

With the exception of HP® blade chassis, generic, IBM®, and Dell® blade chassis are configured on the Port page. The port connected to the blade chassis must be configured with the blade chassis model. The specific information you are able to configure for a blade server will depend on the brand of blade server you are working with. For specific information on each of these supported blade chassis, see their corresponding topics in this section of the help.

The following blade chassis are supported:

- IBM BladeCenter® Models E and H
- Dell PowerEdge® 1855, 1955 and M1000e

A Generic option allows you to configure a blade chassis that is not included in the above list. HP BladeSystem c3000 and c7000 are supported via individual connections from the Dominion device to each blade. The ports are 'grouped' together into a chassis representation using the Port Group Management feature.

Note: Dell PowerEdge 1855/1955 blades also provide the ability to connect from each individual blade to a port on the Dominion device. When connected in that manner, they can also be grouped to create blade server groups.

Two modes of operation are provided for blade chassis: manual configuration and auto-discovery, depending on the blade chassis capabilities. If a blade chassis is configured for auto-discovery, the Dominion device tracks and updates the following:

- When a new blade server is added to the chassis.
- When an existing blade server is removed from the chassis.

Note: In the case of IBM Blade Center Models E and H, the KX II only supports auto-discovery for AMM[1] as the acting primary management module.

The use of hot key sequences to switch KVM access to a blade chassis is also supported. For blade chassis that allow users to select a hot key sequence, those options will be provided on the Port Configuration page. For blade chassis that come with predefined hot key sequences, those sequences will be prepopulated on the Port Configuration page once the blade chassis is selected. For example, the default hot key sequence to switch KVM access to an IBM BladeCenter H is NumLock + NumLock + SlotNumber, so this hot key sequence is applied by default when IBM BladeCenter H is selected during the configuration. See your blade chassis documentation for hot key sequence information.

You are able to configure the connection to a blade chassis web browser interface if one is available. At the chassis level, up to four links can be defined. The first link is reserved for connection to the blade chassis administrative module GUI. For example, this link may be used by technical support to quickly verify a chassis configuration.

Blade chassis can be managed from the Virtual KVM Client (VKC), the Active KVM Client (AKC), Raritan's Multi-Platform Client (MPC), and CC-SG. Managing blade severs via VKC, AKC and MPC is the same as managing standard target servers. See **Working with Target Servers** (on page 37) and the **CC-SG Administrators Guide** for more information. Any changes made to the blade chassis configuration in will be propagated to these client applications.

Important: When the CIM connecting the blade chassis to the Dominion device is powered down or disconnected from the Dominion device, all established connections to the blade chassis will be dropped. When the CIM is reconnected or powered up you will need to re-establish the connection(s).

Important: If you move a blade chassis from one Dominion device port to another Dominion device port, interfaces that were added to the blade chassis node in CC-SG will be lost in CC-SG. All other information will be retained.

Generic Blade Chassis Configuration

The Generic Blade Chassis' selection provides only a manual configuration mode of operation. See ***Supported Blade Chassis Models*** (on page 181), ***Supported CIMs for Blade Chassis*** (on page 182), and ***Required and Recommended Blade Chassis Configurations*** (on page 184) for important, additional information when configuring the blade chassis.

1. Connect the blade chassis to the KX II. See Step 3: Connect the Equipment for details.

2. Select Device Settings > Port Configuration to open the Port Configuration page.
3. On the Port Configuration page, click on the name of the blade chassis you want to configure. The Port page will open.
4. Select the Blade Chassis radio button. The page will then display the necessary fields to configure a blade chassis.
5. Select Generic from the Blade Server Chassis Model drop-down.
6. Configure the blade chassis as applicable.
   a. Switch Hot Key Sequence - Define the hot key sequence that will be used to switch from KVM to the blade chassis. The Switch Hot Key Sequence must match the sequence used by the KVM module in the blade chassis.
   b. Administrative Module Primary IP Address/Host Name - Not applicable.
   c. Maximum Number of Slots - Enter the default maximum number of slots available on the blade chassis.
   d. Port Number - The default port number for the blade chassis is 22. Not applicable.
   e. Username - Not applicable.
   f. Password - Not applicable.
7. Change the blade chassis name if needed.
8. Indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox. If needed, change the blade server names.
9. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available. Click the Blade Chassis Managed Links icon 

to expand the section on the page.

   The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

   Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

   a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.

b. URL - Enter the URL to the interface. Required

c. Username - Enter the username used to access the interface. Optional

d. Password - Enter the password used to access the interface. Optional

Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

e. The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See ***Tips for Adding a Web Browser Interface*** (on page 178) for tips on adding a web browser interface. **Optional**

10. USB profile information does not apply to a generic configuration.
11. In the Target Settings section, select 720x400 Compensation if you are experiencing display issues when the target is using this resolution.
12. Select 'Use international keyboard for scan code set 3' if connecting to the target with a DCIM-PS2 and require the use of scan code set 3 with an international keyboard.
13. Click OK to save the configuration.

Dell Blade Chassis Configuration

See ***Supported Blade Chassis Models*** (on page 181), ***Supported CIMs for Blade Chassis*** (on page 182), and ***Required and Recommended Blade Chassis Configurations*** (on page 184) for important, additional information when configuring the blade chassis. See ***Dell Chassis Cable Lengths and Video Resolutions*** (on page 294) for information on cable lengths and video resolutions when using Dell® chassis with the KX II.

1. Connect the blade chassis to the KX II. See Step 3: Connect the Equipment for details.
2. Select Device Settings > Port Configuration to open the Port Configuration page.
3. On the Port Configuration page, click on the name of the blade chassis you want to configure. The Port page will open.
4. Select the Blade Chassis radio button. The page will then display the necessary fields to configure a blade chassis.

5. Select the Dell blade chassis model from the Blade Server Chassis Model drop-down.

To configure a Dell PowerEdge M1000e:

1. If you selected Dell PowerEdge™ M1000e, auto-discovery is available. Configure the blade chassis as applicable. Prior to configuring a blade chassis that can be auto-discovered, it must be configured to enable SSH connections on the designated port number (see ***Device Services*** (on page 140)). Additionally, a user account with the corresponding authentication credentials must be previously created on the blade chassis.
   a. Switch Hot Key Sequence - Select the hot key sequence that will be used to switch from KVM to the blade server. The Switch Hot Key Sequence must match the sequence used by the KVM module in the blade chassis.
   b. Maximum Number of Slots - The default maximum number of slots available on the blade chassis is automatically entered.
   c. Administrative Module Primary IP Address/Host Name - Enter the primary IP address for the blade chassis. **Required for auto-discovery mode**
   d. Port Number - The default port number for the blade chassis is 22. Change the port number if applicable. **Required for auto-discovery mode**
   e. Username - Enter the username used to access the blade chassis. **Required for auto-discovery mode**
   f. Password - Enter the password used to access the blade chassis. **Required for auto-discovery mode**
2. If you want the KX II to auto-discover the chassis blades, select the Blade Auto-Discovery checkbox and then click the Discover Blades on Chassis Now button. Once the blades are discovered, they will be displayed on the page.
3. Change the blade chassis name if needed. If the chassis is already named, that information automatically populates this field. If it is not already named, the KX II assigns the chassis a name. The default naming convention for the blade chassis by the KX II is # Blade_Chassis_Port#.
4. If operating in Manual mode, indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox. If needed, change the blade server names

   If operating in Auto-discovery mode, the Installed box will display the slots containing blades during discovery.

5. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available. Click the Blade Chassis Managed Links icon 

to expand the section on the page.

   The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

   Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

   a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.

   b. URL - Enter the URL to the interface. See ***Blade Chassis Sample URL Formats*** (on page 186) for sample configurations for the Dell M1000e.

   c. Username - Enter the username used to access the interface.

   d. Password - Enter the password used to access the interface.

   Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

   e. The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See ***Tips for Adding a Web Browser Interface*** (on page 178) for tips on adding a web browser interface.

6. USB profiles do not apply to Dell chassis.

7. In the Target Settings section, select 720x400 Compensation if you are experiencing display issues when the target is using this resolution.

8. Select 'Use international keyboard for scan code set 3' if connecting to the target with a DCIM-PS2 and require the use of scan code set 3 with an international keyboard.

9. Click OK to save the configuration.

To configure a Dell PowerEdge 1855/1955:

1. If you selected Dell 1855/1955, auto-discovery *is not available*. Configure the blade chassis as applicable.
   a. Switch Hot Key Sequence - Select the hot key sequence that will be used to switch from KVM to the blade server.
   b. Maximum Number of Slots - The default maximum number of slots available on the blade chassis is automatically entered.
   c. Administrative Module Primary IP Address/Host Name - Not applicable.
   d. Port Number - The default port number for the blade chassis is 22. Not applicable.
   e. Username - Not applicable.
   f. Password - Not applicable.
2. Change the blade chassis name if needed.
3. Indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox. If needed, change the blade server names.
4. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available. Click the Blade Chassis Managed Links icon 

to expand the section on the page.

   The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

   Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

   a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.
   b. URL - Enter the URL to the interface. See ***Blade Chassis Sample URL Formats*** (on page 186) for sample configurations for the Dell PowerEdge 1855/1955.
   c. Username - Enter the username used to access the interface.
   d. Password - Enter the password used to access the interface.

Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

e. The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See ***Tips for Adding a Web Browser Interface*** (on page 178) for tips on adding a web browser interface.

5. USB profiles do not apply to Dell chassis.
6. Click OK to save the configuration.

IBM Blade Chassis Configuration

See ***Supported Blade Chassis Models*** (on page 181), ***Supported CIMs for Blade Chassis*** (on page 182), and ***Required and Recommended Blade Chassis Configurations*** (on page 184) for important, additional information when configuring the blade chassis.

1. Connect the blade chassis to the KX II. See Step 3: Connect the Equipment for details.
2. Select Device Settings > Port Configuration to open the Port Configuration page.
3. On the Port Configuration page, click on the name of the blade chassis you want to configure. The Port page will open.
4. Select the Blade Chassis radio button. The page will then display the necessary fields to configure a blade chassis.
5. Select the IBM® blade chassis model from the Blade Server Chassis Model drop-down.

To configure a IBM BladeCenter H and E:

1. If you selected IBM BladeCenter® H or E, auto-discovery is available. Configure the blade chassis as applicable. Prior to configuring a blade chassis that can be auto-discovered, it must be configured to enable SSH connections on the designated port number (see ***Device Services*** (on page 140)). Additionally, a user account with the corresponding authentication credentials must be previously created on the blade chassis. The KX II only supports auto-discovery for AMM[1].

   a. Switch Hot Key Sequence - Predefined.

   b. Maximum Number of Slots - The default maximum number of slots available on the blade chassis is automatically entered.

c. Administrative Module Primary IP Address/Host Name - Enter the primary IP address for the blade chassis. **Required for auto-discovery mode**

d. Port Number - The default port number for the blade chassis is 22. Change the port number if applicable. **Required for auto-discovery mode**

e. Username - Enter the username used to access the blade chassis. **Required for auto-discovery mode**

f. Password - Enter the password used to access the blade chassis. **Required for auto-discovery mode**

2. If you want the KX II to auto-discover the chassis blades, select the Blade Auto-Discovery checkbox and then click the Discover Blades on Chassis Now button. Once the blades are discovered, they will be displayed on the page.

3. Change the blade chassis name if needed. If the chassis is already named, that information automatically populates this field. If it is not already named, the KX II assigns the chassis a name. The default naming convention for the blade chassis by the KX II is # Blade_Chassis_Port#.

4. If operating in Manual mode, indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox. If needed, change the blade server names

   If operating in Auto-discovery mode, the Installed box will display the slots containing blades during discovery.

5. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available. Click the Blade Chassis Managed Links icon 

to expand the section on the page.

   The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

   Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

   a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.

   b. URL - Enter the URL to the interface. See ***Blade Chassis Sample URL Formats*** (on page 186) for sample configurations for the IBM BladeCenter.

c. Username - Enter the username used to access the interface.

d. Password - Enter the password used to access the interface.

Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

e. The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See ***Tips for Adding a Web Browser Interface*** (on page 178) for tips on adding a web browser interface.

6. If applicable, define the USB profile for the blade chassis or select an existing USB profile. Click the USB Profiles Select USB Profiles for Port icon 

or the Apply Select Profiles to Other Ports icon 

to expand these sections of the page. See ***Configuring USB Profiles (Port Page)*** (on page 187).

7. Click OK to save the configuration.

To configure a IBM BladeCenter (Other):

1. If you selected IBM BladeCenter (Other), auto-discovery *is not* available. Configure the blade chassis as applicable.

   a. Switch Hot Key Sequence - Select the hot key sequence that will be used to switch from KVM to the blade server.

   b. Administrative Module Primary IP Address/Host Name - Enter the primary IP address for the blade chassis. Not applicable.

   c. Maximum Number of Slots - Enter the default maximum number of slots available on the blade chassis.

   d. Port Number - The default port number for the blade chassis is 22. Not applicable.

   e. Username - Not applicable.

   f. Password - Not applicable.

2. Change the blade chassis name if needed.

3. Indicate the blades that are installed in the blade chassis by checking the Installed checkbox next to each slot that has a blade installed. Alternatively, use the Select All checkbox. If needed, change the blade server names. If it is not already named, the KX II assigns a name to the blade server. The default blade server naming convention is # Blade_Chassis_Port#_Slot#.

4. In the Blade Chassis Managed Links section of the page, you are able to configure the connection to a blade chassis web browser interface if one is available. Click the Blade Chassis Managed Links icon 

to expand the section on the page.

   The first URL link is intended for use to connect to the blade chassis Administration Module GUI.

   Note: Access to the URL links entered in this section of the page is governed by the blade chassis port permissions.

   a. Active - To activate the link once it is configured, select the Active checkbox. Leave the checkbox deselected to keep the link inactive. Entering information into the link fields and saving can still be done even if Active is not selected. Once Active is selected, the URL field is required. The username, password, username field and password field are optional depending on whether single sign-on is desired or not.

   b. URL - Enter the URL to the interface. See ***Blade Chassis Sample URL Formats*** (on page 186) for sample configurations for the IBM BladeCenter.

   c. Username - Enter the username used to access the interface.

   d. Password - Enter the password used to access the interface.

   Note: Leave the username and password fields blank for DRAC, ILO, and RSA web applications or the connection will fail.

   e. The Username Field and Password Field, which are both optional, contain the labels that are expected to be associated with the username and password entries. It is in these fields you should enter the field names for the username and password fields used on the login screen for the web application. You can view the HTML source of the login screen to find the field *names*, not the field labels. See ***Tips for Adding a Web Browser Interface*** (on page 178) for tips on adding a web browser interface.

5. USB profiles are not used by IBM (Other) configurations.

6. In the Target Settings section, select 720x400 Compensation if you are experiencing display issues when the target is using this resolution.

7. Select 'Use international keyboard for scan code set 3' if connecting to the target with a DCIM-PS2 and require the use of scan code set 3 with an international keyboard.

8. Click OK to save the configuration.

Tips for Adding a Web Browser Interface

You can add a Web Browser Interface to create a connection to a device with an embedded web server. A Web Browser interface can also be used to connect to any web application, such as the web application associated with an RSA, DRAC or ILO Processor card.

You must have DNS configured or URLs will not resolve. You do not need to have DNS configured for IP addresses.

To add a web browser interface:

1. The default name for a Web Browser Interface is provided. If needed, change the name in the Name field.
2. Enter the URL or domain name for the web application in the URL field. You must enter the URL at which the web application expects to read the username and password.

   Follow these examples for correct formats:

   - http(s)://192.168.1.1/login.asp
   - http(s)://www.example.com/cgi/login
   - http(s)://example.com/home.html
3. Enter the username and password that will allow access to this interface. **Optional**
4. If username and password were entered, in the Username Field and Password Field, type the field names for the username and password fields that are used in the login screen for the web application. You must view the HTML source of the login screen to find the field names, not the field labels.

Tip for locating field names:

- In the HTML source code for the login page of the web application, search for the field's label, such as Username and Password.
- When you find the field label, look in the adjacent code for a tag that looks like this: name="user". The word in quotes is the field name.

HP Blade Chassis Configuration (Port Group Management)

The KX II supports the aggregation of ports connected to certain types of blades into a group representing the blade chassis. Specifically, HP® BladeServer blades and Dell® PowerEdge™ 1855/1955 blades when the Dell PowerEdge 1855/1955 is connected from each individual blade to a port on the KX II.

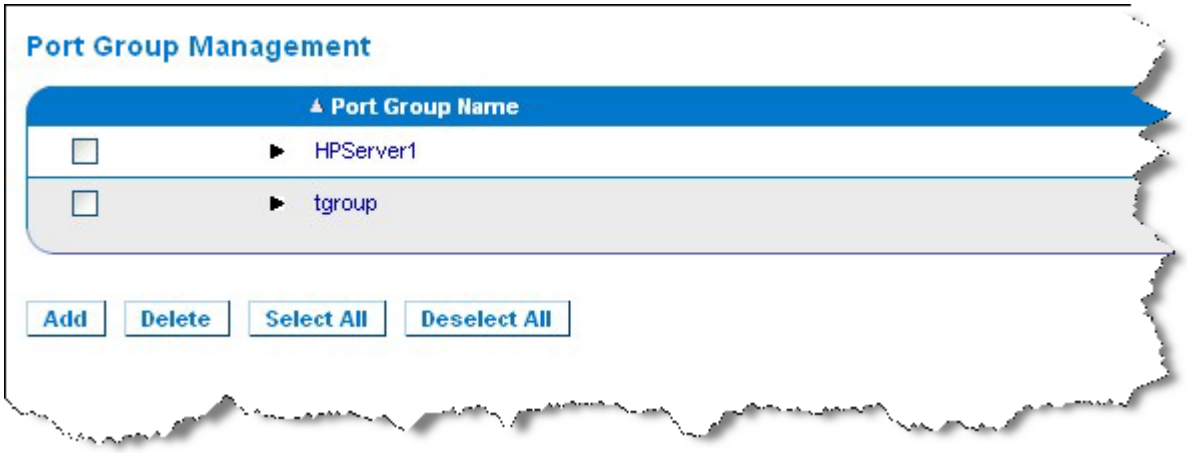
The chassis is identified by a Port Group Name and the group is designated as a Blade Server Group on the Port Group Management page. Port Groups consist solely of ports configured as standard KVM ports, not ports configured as blade chassis. A port may only be a member of a single group.

Ports connected to integrated KVM modules in a blade chassis are configured as blade chassis subtypes. These ports are eligible to be included in port groups.

When KX II ports are connected to integrated KVM modules in a blade chassis and not to individual blades, the ports are configured as blade chassis subtypes. These ports are not eligible to be included in port groups and will not appear in the Select Port for Group, Available list.

If a standard KVM port has been included in a port group, and then is subsequently repurposed for use as a blade chassis subtype, it must first be removed from the port group.

Port Groups are restored using the Backup and Restore option (see ***Backup and Restore*** (on page 213)).



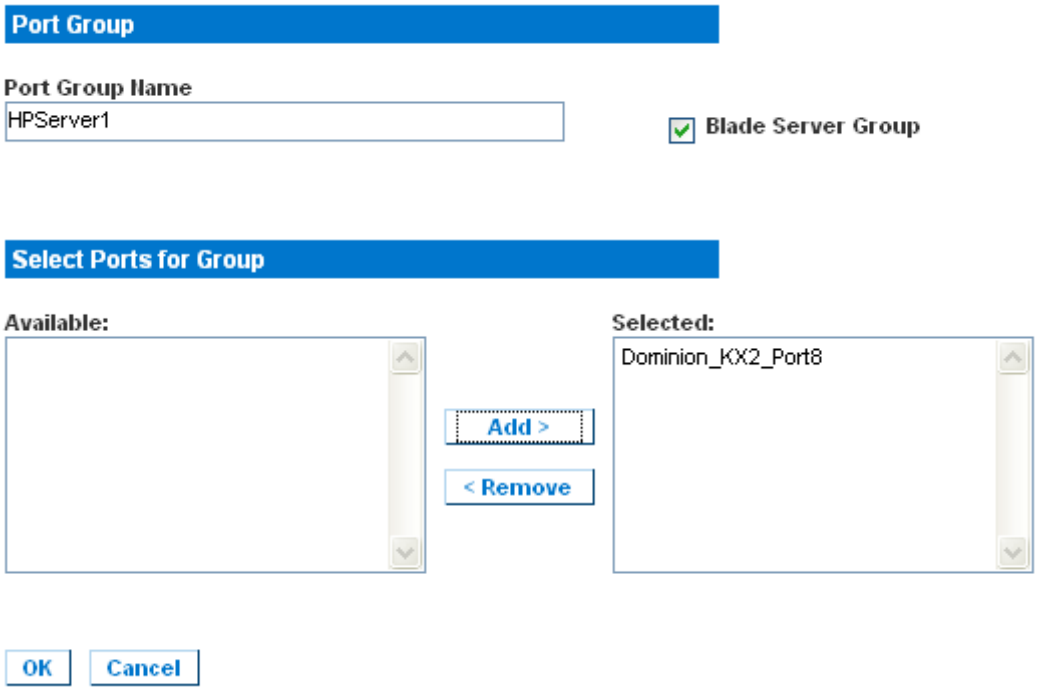
To add a port group:

1. Click Device Settings > Port Group Management to open the Port Group Management page.
2. Click the Add button to open the Port Group page.

3. Enter a Port Group Name. The port group name is not case sensitive and can contain up to 32 characters.
4. Select the Blade Server Group checkbox.

   If you want to designate that these ports are attached to blades housed in a blade chassis (for example, HP c3000 or Dell PowerEdge 1855), select the Blade Server Group checkbox.

   Note: This is especially important to CC-SG users who want HP blades to be organized on a chassis basis, although each blade has its own connection to a port on the KX II.
5. Click on a port in the Available box in the Select Ports for Group section. Click Add to add the port to the group. The port will be moved to the Selected box.
6. Click OK to add the port group.



To edit port group information:

1. On the Port Group Management page, click on the link of the port group you want to edit. The Port Group page opens.
2. Edit the information as needed.
3. Click OK to save the changes.

To delete a port group:

1. Click on the Port Group Management page, select the checkbox of the port group you want to delete.
2. Click the Delete button.
3. Click OK on the warning message.

Supported Blade Chassis Models

This table contains the blade chassis models that are supported by the KX II and the corresponding profiles that should be selected per chassis model when configuring them in the KX II application. A list of these models can be selected on the Port Configuration page from the Blade Server Chassis Model drop-down, which appears when the Blade Chassis radio button is selected. For details on how to configure each blade chassis model, see their corresponding topics in this section of the help.

Blade chassis model	KX II Profile
Dell® PowerEdge™ 1855/1955	Dell PowerEdge 1855/1955
Dell PowerEdge M1000e	Dell PowerEdge M1000e
IBM® BladeCenter® S	IBM (Other)
IBM BladeCenter H	IBM BladeCenter H
IBM BladeCenter T	IBM (Other)
IBM BladeCenter HT	IBM (Other)
IBM BladeCenter E	IBM BladeCenter E
HP®	Configure using Port Group Management functions. See ***HP Blade Chassis Configuration (Port Group Management)*** (on page 179).

Supported CIMs for Blade Chassis

The following CIMs are supported for blade chassis being managed through the KX II:

- DCIM-PS2
- DCIM-USBG2
- D2CIM-VUSB
- D2CIM-DVUSB

Following is a table containing supported CIMs for each blade chassis model that the KX II supports.

Blade chassis	Connection method	Recommended CIM(s)
Generic	If a D2CIM-VUSB or D2CIM-DVUSB is used when connecting to a blade-chassis configured as Generic, you will be able to select the USB profiles from the Port Configuration page and the client's USB Profile menu. However, virtual media is not supported for generic blade chassis and the Virtual Media menu is disabled on the client.	• DCIM-PS2 • DCIM-USBG2
Dell® PowerEdge™ 1855	Includes one of the three KVM modules : • Analog KVM Ethernet switch module (standard) • Digital Access KVM switch module (optional) • KVM switch module (standard on systems sold prior to April, 2005) These switches provide a custom connector that allows two PS/2 and one video device to be connected to the system. Source: *Dell PowerEdge 1855 User Guide*	• DCIM-PS2
Dell PowerEdge 1955	One of two types of KVM modules may be installed: • Analog KVM switch module • Digital Access KVM switch module Both modules enable you to connect a PS/2-compatible keyboard, mouse and video monitor to the system (using a custom cable provided with the system). Source: *Dell PowerEdge 1955 Owner's Manual*	• DCIM-PS2
Dell PowerEdge	The KVM Switch Module (iKVM) is Integrated	• DCIM-USBG2

Blade chassis	Connection method	Recommended CIM(s)
M1000e	with this chassis. The iKVM is compatible with the following peripherals: • USB keyboards, USB pointing devices • VGA monitors with DDC support. Source: *Dell Chassis Management Controller, Firmware Version 1.0, User Guide*	
HP® BladeSystem c3000	The HP c-Class Blade SUV Cable enables you to perform blade chassis administration, configuration, and diagnostic procedures by connecting video and USB devices directly to the server blade. Source: *HP Proliant™ BL480c Server Blade Maintenance and Service Guide*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (for standard KVM port operation without a KVM option)
HP BladeSystem c7000	The HP c-Class Blade SUV Cable enables you to perform server blade administration, configuration, and diagnostic procedures by connecting video and USB devices directly to the server blade. Source: *HP ProLiant BL480c Server Blade Maintenance and Service Guide*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (for standard KVM port operation)
IBM® BladeCenter® S	The Advanced Management Module (AMM) provides system management functions and keyboard/video/mouse (KVM) multiplexing for all blade chassis. The AMM connections include: a serial port, video connection, remote management port (Ethernet), and two USB v2.0 ports for a keyboard and mouse. Source: *Implementing the IBM BladeCenter S Chassis*	• DCIM-USBG2
IBM BladeCenter H	The BladeCenter H chassis ships standard with one Advanced Management Module. Source: *IBM BladeCenter Products and Technology*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter E	The current model BladeCenter E chassis (8677-3Rx) ships standard with one Advanced Management Module. Source: *IBM BladeCenter Products and Technology*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	The BladeCenter T chassis ships standard with	• DCIM-PS2

Blade chassis	Connection method	Recommended CIM(s)
	one Advanced Management Module. In contrast to the standard BladeCenter chassis, the KVM module and the Management Module in the BladeCenter T chassis are separate components. The front of the Management Module only features the LEDs for displaying status. All Ethernet and KVM connections are fed through to the rear to the LAN and KVM modules. The KVM module is a hot swap module at the rear of the chassis providing two PS/2 connectors for keyboard and mouse, a systems-status panel, and a HD-15 video connector. Source: *IBM BladeCenter Products and Technology*	
IBM BladeCenter HT	The BladeCenter HT chassis ships standard with one Advanced Management Module. This module provides the ability to manage the chassis as well as providing the local KVM function. Source: *IBM BladeCenter Products and Technology*	• DCIM-USBG2

Note: In order to support Auto-discovery, IBM BladeCenter Models H and E must use AMM with firmware version BPET36K or later.

Note: In the case of IBM Blade Center Models E and H, the KX II only supports auto-discovery for AMM[1] as the acting primary management module.

Required and Recommended Blade Chassis Configurations

This table contains information on limitations and constraints that apply to configuring blade chassis to work with the KX II. Raritan recommends that all of the information below is followed.

Blade chassis	Required/recommended action
Dell® PowerEdge™ M1000e	• Disable the iKVM GUI screensaver. An authorize dialog will appear, preventing iKVM from working correctly, if this is not done. • Exit the iKVM GUI menu before attaching Dell's chassis to a Raritan CIM. iKVM may not work correctly if this is not done. • Configure the iKVM GUI Main menu to select target blades by

Blade chassis	Required/recommended action
	Slot, not by Name. iKVM may not work correctly if this is not done. • *Do not* designate any slots for scan operations in the iKVM GUI Setup Scan menu. iKVM may not work correctly otherwise. • *Do not* designate any slots for broadcast keyboard/mouse operations in the iKVM GUI Setup Broadcast menu. iKVM may not work correctly otherwise. • Designate a single key sequence to invoke the iKVM GUI. This key sequence must also be identified during KX II port configuration. Otherwise, indiscriminate iKVM operation may occur as a result of client key entry. • Ensure that Front Panel USB/Video Enabled is *not* selected during iKVM configuration via the Dell CMC GUI. Otherwise, connections made at the front of chassis will take precedence over the KX II connection at the rear, preventing proper iKVM operation. A message will be displayed stating 'User has been disabled as front panel is currently active.' • Ensure that 'Allow access to CMC CLI from iKVM' is *not* selected during iKVM configuration via the Dell CMC GUI. • To avoid having the iKVM GUI display upon connecting to the blade chassis, set the Screen Delay Time to 8 seconds. • Recommend that 'Timed' and 'Displayed' be selected during iKVM GUI Flag Setup. This will allow you to visually confirm the connection to the desired blade slot.
Dell PowerEdge 1855/1955	• Disable the iKVM GUI screensaver. An Authorize dialog will appear if this is not done and will prevent the iKVM from operating correctly. • Exit the iKVM GUI menu before attaching Dell's chassis to a Raritan CIM. iKVM may not work correctly if this is not done. • Configure the iKVM GUI Main menu to select target blades by Slot, not by Name. iKVM may not work correctly if this is not done. • *Do not* designate any slots for scan operations in the iKVM GUI Setup Scan menu or the iKVM may not work properly. • To avoid having the iKVM GUI display upon connecting to the blade chassis, set the Screen Delay Time to 8 seconds. • Recommend that 'Timed' and 'Displayed' be selected during iKVM GUI Flag Setup. This will allow you to visually confirm the connection to the desired blade slot.
IBM®/Dell® Auto-Discovery	• It is recommended that Auto-Discovery be enabled when applying blade level access permissions. Otherwise, set access permissions on a blade-chassis wide basis. • Secure Shell (SSH) must be enabled on the blade chassis

Blade chassis	Required/recommended action
	management module. • The SSH port configured on the blade chassis management module and the port number entered on the Port Configuration page must match.
IBM KX2 Virtual Media	• Raritan KX II virtual media is supported only on IBM BladeCenter® Models H and E. This requires the use of the D2CIM-DVUSB. The black D2CIM-DVUSB Low-Speed USB connector is attached to the Administrative Management Module (AMM) at the rear of the unit. The gray D2CIM-DVUSB High-Speed USB connector is attached to the Media Tray (MT) at the front of the unit. This will require a USB extension cable.

Note: All IBM BladeCenters that use AMM must use AMM firmware version BPET36K or later to work with the KX II.

Note: In the case of IBM Blade Center Models E and H, the KX II only supports auto-discovery for AMM[1] as the acting primary management module.

Blade Chassis Sample URL Formats

This table contains sample URL formats for blade chassis being configured in the KX II.

Blade chassis	Sample URL format
Dell® M1000e	• URL: https://192.168.60.44/cgi-bin/webcgi/login • Username: root • Username Field: user • Password: calvin • Password Field: password
Dell 1855	• URL: https://192.168.60.33/Forms/f_login • Username: root • Username Field: TEXT_USER_NAME • Password: calvin • Password Field: TEXT_PASSWORD
IBM® BladeCenter® E or H	• http://192.168.84.217/private/welcome.ssi

Configuring 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® operating system, Windows XP® operating system, Windows Vista® operating system profile. For information about USB profiles, see ***USB Profiles*** (on page 101).

Note: To set USB profiles for a port, you must have a VM-CIM or Dual VM-CIM connected with firmware compatible with the current firmware version of the KX II. See **Upgrading CIMs** *(on page 217).*

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 its 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.

Note: See **Mouse Modes when Using the Mac OS-X USB Profile with a DCIM-VUSB** *(on page 109) for information on using the Mac OS-X® USB profile if you are using a DCIM-VUSB or DCIM-DVUSB.*

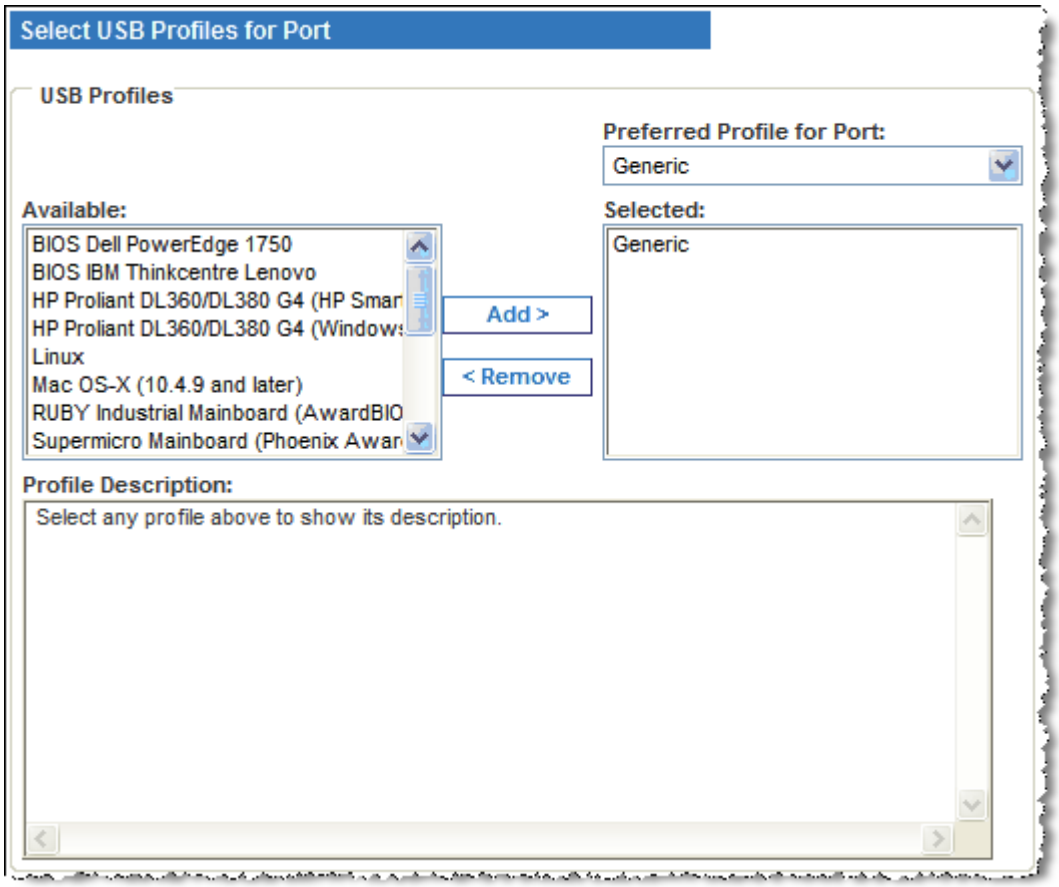
To open the Port page:

1. Choose Device Settings > Port Configuration. The Port Configuration page opens.
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.



2. Click Add. The selected profiles appear in the Selected list. These are the profiles that can be used 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.

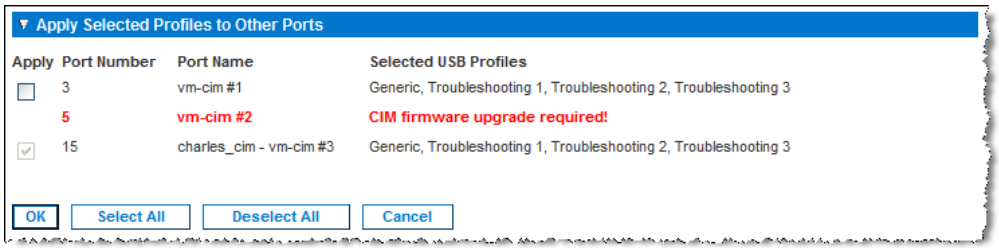
To remove selected USB profiles:

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.



- To select all KVM ports, click Select All.
- To deselect all KVM ports, click Deselect All.

Configuring KX II Local Port Settings

From the Local Port Settings page, you can customize many settings for the KX II Local Console including keyboard, hot keys, video switching delay, power save mode, local user interface resolution settings, and local user authentication. Further, you can change a USB profile from the local port.

For the KX2-832 and KX2-864, you are also able to configure the extended local port from the Local Port Settings page. The extended local port may be connected to a Paragon switch or User Station to extend the reach of the Local port. Like the standard local port, you are able configure keyboard, hot keys, video switching delay, power save mode, local user interface resolution settings, and local user authentication settings. The extended local port can be configured from both the Remote Console and the Local Console. See ***KX2-832 and KX2-864 Standard and Extended Local Port Settings*** (on page 194) for more information on the standard local port and extended local port.

Note: If the extended local port is enabled on the KX2-832 and KX2-864 and nothing is connected to the port, you will experience a delay of 2-3 seconds when switching to a target via the local port.

To configure the local port settings:

Note: Some changes you make to the settings on the Local Port Settings page will restart the browser you are working in. If a browser restart will occur when a setting is changed, it is noted in the steps provider here.

1. Choose Device Settings > Local Port Settings. The Local Port Settings page opens.
2. Select the checkbox next to the Enable Standard Local Port to enable it. Deselect the checkbox to disable it. By default, the standard local port is enabled but can be disabled as needed. The browser will be restarted when this change is made. If you are using the tiering feature, this feature will be turned off since both features cannot be used at the same time.
3. If you are using a KX2-832 or KX2-864 device, select the checkbox next to the Extended Local Port to enable it. Deselect the checkbox(s) to disable it. If you are using the smart card feature, the extended local port be must be disabled. The browser will be restarted when this change is made.

   If both the standard local port and extended local port are disabled, the local ports cannot be accessed. If you attempt to access a KX2-832 or KX2-864 through a disabled local port, a message will be displayed indicating that the device is under remote management and that the login is disabled.

Note: If you are using KX2-832 and KX2-864 as tiered devices, you must connect them to the base KX II via the extended local port.

Note: If you connect a Paragon device to the KX2-832 and KX2-864 extended local port, you must use the remote client to change the USB profile.

4. If you are using the tiering feature, select the Enable Local Port Device Tiering checkbox and enter the tiered secret word in the Tier Secret field. In order to configure tiering, you must also configure the base device on the Device Services page. See ***Configuring and Enabling Tiering*** (on page 142) for more information on tiering.
5. Choose the appropriate keyboard type from among the options in the drop-down list. The browser will be restarted when this change is made.
   - US
   - US/International
   - United Kingdom
   - French (France)
   - German (Germany)
   - JIS (Japanese Industry Standard)
   - Simplified Chinese
   - Traditional Chinese
   - Dubeolsik Hangul (Korean)
   - German (Switzerland)
   - Portuguese (Portugal)
   - Norwegian (Norway)
   - Swedish (Sweden)
   - Danish (Denmark)
   - Belgian (Belgium)

Note: Keyboard use for Chinese, Japanese, and Korean is for display only. Local language input is not supported at this time for KX II Local Console functions.

6. Choose the local port hotkey. The local port hotkey is used to return to the 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

Hot key:	Take this action:
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

7. Select the Local Port Connect key. Use a connect key sequence to connect to a target and switch to another target. You can then use the hot key to disconnect from the target and return to the local port GUI. The connect key works for both standard servers and blade chassis. Once the local port connect key is created, it will appear in the Navigation panel of the GUI so you can use it as a reference. See ***Connect Key Examples*** (on page 249) for examples of connect key sequences.
8. 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).
9. 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.
10. Choose the resolution for the KX II Local Console from the drop-down list. The browser will be restarted when this change is made.
    - 800x600
    - 1024x768
    - 1280x1024
11. Choose the refresh rate from the drop-down list. The browser will be restarted when this change is made.
    - 60 Hz
    - 75 Hz
12. Choose the type of local user authentication.
    - Local/LDAP/RADIUS. This is the recommended option. For more information about authentication, see ***Remote Authentication*** (on page 34).
    - None. There is no authentication for Local Console access. This option is recommended for secure environments only.

- Select the "Ignore CC managed mode on local port" checkbox if you would like local user access to the KX II even when the device is under CC-SG management.

Note: If you initially choose not 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.

Note: In order to use the standard local port and extended local port while the KX II is under CC-SG management, "Ignore CC managed mode on local port" option must be selected. Select the "Ignore CC managed mode on local port" checkbox if you would like local user access, via the standard or extended local port, to the KX II when the device is under CC-SG management. Alternatively, use the direct device access while under CC-SG management feature.

---

13. Click OK.

KX2-832 and KX2-864 Standard and Extended Local Port Settings

The KX2-832 and KX2-864 provides you with two local port options: the standard local port and the extended local port. Each of these port options is enabled and disabled from the Remote Console on the Port Configuration page or from the Local Console on the Local Port Settings page. For more information, see ***Configuring KX II Local Port Settings*** (on page 190).

By default, the standard local port is enabled and the extended local port is disabled. If you would like to extend the reach of the local port, enable the extended local port and use a Cat5/5e/6 cable to connect to the DKX2-832 or DKX2-864 from a Paragon II UMT, EUST, UST or URKVMG.

Note: If the extended local port is enabled on the KX2-832 and KX2-864 and nothing is connected to the port, you will experience a delay of 2-3 seconds when switching to a target via the Local port.

You must have Administrator privileges to configure these options. To access a port, you only need to enter your username and password once. You do not have to enter these credentials for each port you access.

See the ***Specifications*** (on page 257) section for details on the devices supported by the extended local port, as well as distance specifications and supported CIMs.

KX2-832 and KX2-864 Connection Limitations

The standard and extended local ports share access to a target. When both are enabled, the keyboard, video and mouse are shared between the standard and extended local ports. Both will be connected to or disconnected from the target.

When either the standard or extended local ports is disabled, the keyboard, video and mouse for the ports will be disabled and a message is displayed you that the local ports have been disabled.

Port Group Management

This function is specific to HP blade chassis configuration. See ***HP Blade Chassis Configuration (Port Group Management)*** (on page 179).

Chapter 9 Security Management

In This Chapter

Security Settings

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

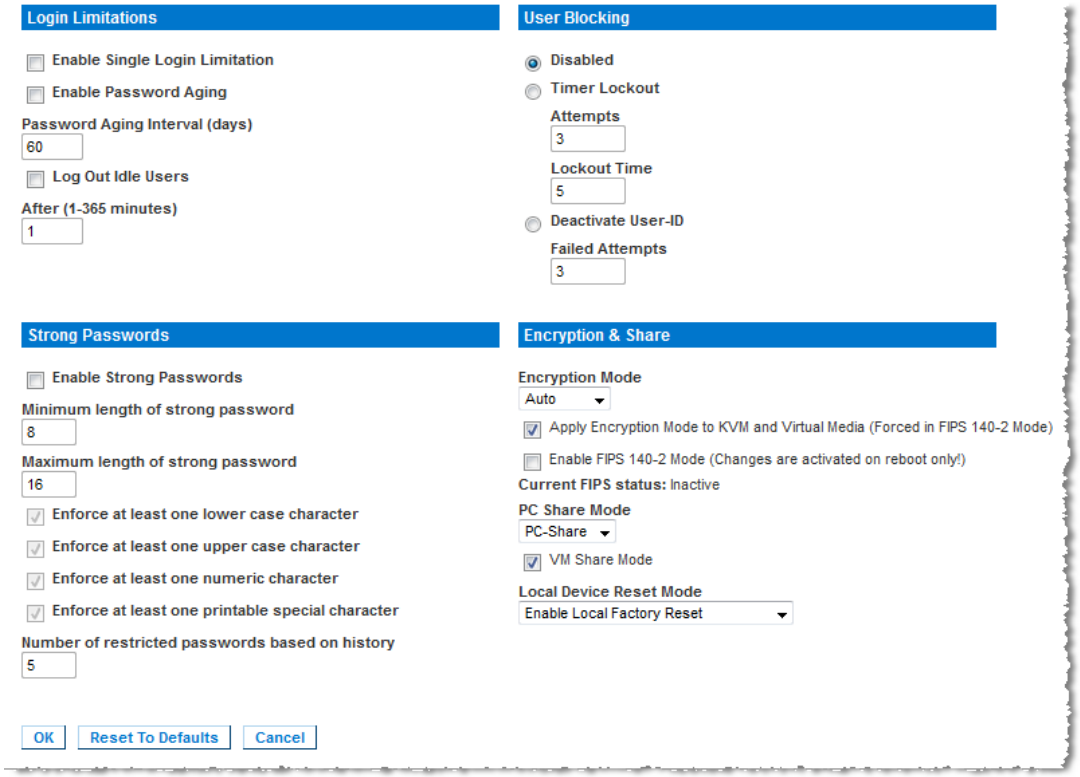
Raritan SSL certificates are used for public and private key exchanges, and provide an additional level of security. Raritan web server certificates are self-signed. Java applet certificates are signed by a VeriSign certificate. Encryption guarantees that your information is safe from eavesdropping and 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.
2. Update the ***Login Limitations*** (on page 196) settings as appropriate.
3. Update the ***Strong Passwords*** (on page 198) settings as appropriate.
4. Update the ***User Blocking*** (on page 199) settings as appropriate.
5. Update the Encryption & Share settings as appropriate.
6. Click OK.

To reset back to defaults:

- Click Reset to Defaults.

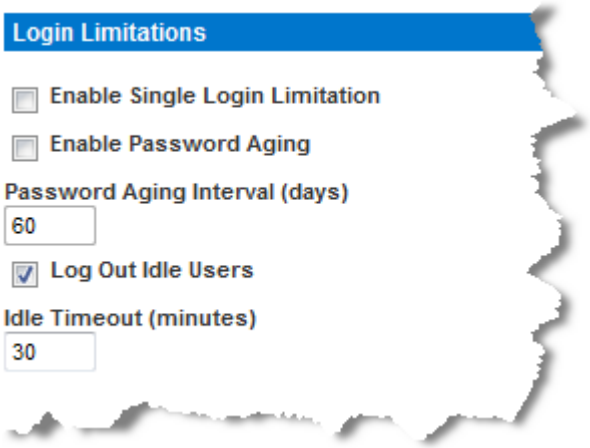


Login Limitations

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

Limitation	Description
Enable single login 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.

Limitation	Description
	Enter the number of days after which a password change is required. The default is 60 days.
Log out idle users, After (1-365 minutes)	Select the "Log off idle users" checkbox to automatically disconnect users after the amount of time you specify in the "After (1-365 minutes)" field. If there is no activity from the keyboard or mouse, all sessions and all resources are logged out. If a virtual media session is in progress, however, the session does not timeout. The After field is used to set the amount of time (in minutes) after which an idle user will be logged out. This field is enabled when the Log Out Idle Users option is selected. Up to 365 minutes can be entered as the field value



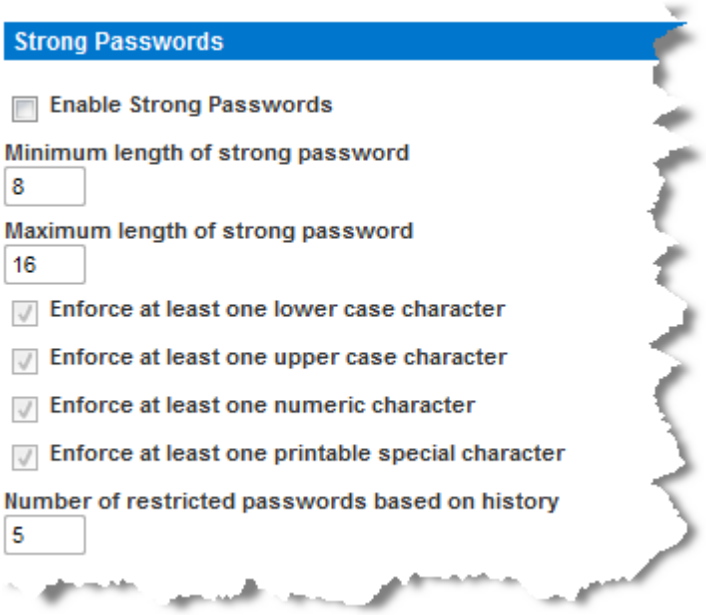
Strong Passwords

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

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 8 minimum and 16 the is the default maximum.
Enforce at least one lower case character	When checked, at least one lower case character is required in the password.
Enforce at least one upper case character	When checked, at least one upper case character is required in the password.
Enforce at least one numeric character	When checked, at least one numeric character is required in the password.
Enforce at least one printable special character	When checked, at least one special character (printable) is required in the password.
Number of restricted passwords based on history	This field represents the password history depth. That is, the number of prior passwords that cannot be repeated. The range is 1-12 and the default is 5.



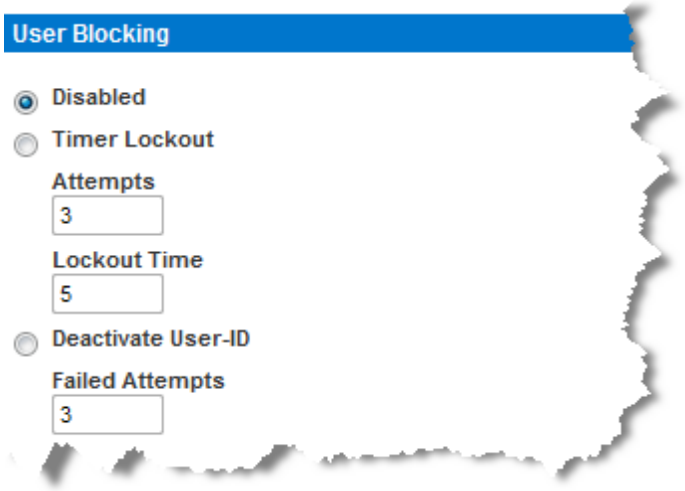
User Blocking

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.

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 and 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 and the default is 5 minutes. *Note: Users in the role of Administrator are exempt from the timer lockout settings.*
Deactivate User-ID	When selected, this option specifies that the user will be locked out of the system after the number of failed login attempts specified in the Failed Attempts field: ▪ Failed Attempts - The number of unsuccessful login attempts after which the user's User-ID will be deactivated. This field is enabled when the Deactivate User-ID option is selected. The valid range is 1 - 10. 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.



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 KX II Reset button is pressed.

WARNING: If you select an encryption mode that is not supported by your browser, you will not be able to access the KX II from your browser.

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

Encryption mode	Description
Auto	This is the recommended option. The KX II autonegotiates to the highest level of encryption possible. You *must* select Auto in order for the device and client to successfully negotiate the use of FIPS compliant algorithms.
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 KX II device and the Remote PC during initial connection authentication. If you enable FIPS 140-2 mode and RC4 has been selected, you will receive an error message. RC4 is not available while in FIPS 140-2 mode.
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. See ***Checking Your Browser for AES Encryption*** (on page 203) for more information.
AES-256	The Advanced Encryption Standard (AES) is

Encryption mode	Description
	a National Institute of Standards and Technology specification for the encryption of electronic data. 256 is the key length. When AES-256 is specified, be certain that your browser supports it, otherwise you will not be able to connect. See ***Checking Your Browser for AES Encryption*** (on page 203) for more information.

Note: MPC will always negotiate to the highest encryption and will match the Encryption Mode setting if not set to Auto.

Note: If you are running Windows XP® operating system with Service Pack 2, Internet Explorer® 7 cannot connect remotely to the KX II using AES-128 encryption.

2. 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.
3. For government and other high security environments, enable FIPS 140-2 Mode by selecting the Enable FIPS 140-2 checkbox. See ***Enabling FIPS 140-2*** (on page 204) for information on enabling FIPS 140-2.
4. PC Share Mode. Determines global concurrent remote KVM access, enabling up to eight remote users to simultaneously log into one 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.
5. If needed, select 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.
6. If needed, select Local Device Reset Mode. This option specifies which actions are taken when the hardware Reset button (at the back of the device) is depressed. For more information, see Resetting the KX II Using the Reset Button. Choose one of the following options:

Local device reset mode	Description
Enable Local Factory Reset (default)	Returns the KX II device 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.

Note: When using the P2CIM-AUSBDUAL or P2CIM-APS2DUAL to attach a target to two KX IIs, if Private access to the targets is required, both KVM switches must have Private set as their PC Share Mode.

See Supported Paragon CIMS and Configurations for additional information on using Paragon CIMs with the KX II.

Checking Your Browser for AES Encryption

The KX II supports AES-256. 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: Internet Explorer® 6 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 and 3.0.x and higher
- Internet Explorer 7 and 8

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 JREs™ are available at the “other downloads” section of the following link:

- JRE1.6 - http://java.sun.com/javase/downloads/index_jdk5.jsp

Enabling FIPS 140-2

For government and other high security environments, enabling FIPS 140-2 mode may be desirable. The KX II uses an embedded FIPS 140-2-validated cryptographic module running on a Linux® platform per FIPS 140-2 Implementation Guidance section G.5 guidelines. Once this mode is enabled, the private key used to generate the SSL certificates must be internally generated; it cannot be downloaded or exported.

To enable FIPS 140-2:

1. Access the Security Settings page.
2. Enable FIPS 140-2 Mode by selecting the Enable FIPS 140-2 checkbox in the Encryption & Share section of the Security Settings page. You will utilize FIPS 140-2 approved algorithms for external communications once in FIPS 140-2 mode. The FIPS cryptographic module is used for encryption of KVM session traffic consisting of video, keyboard, mouse, virtual media and smart card data.
3. Reboot the KX II. **Required**

   Once FIPS mode is activated, 'FIPS Mode: Enabled' will be displayed in the Device Information section in the left panel of the screen.

   For additional security, you can also create a new Certificate Signing Request once FIPS mode is activated. This will be created using the required key ciphers. Upload the certificate after it is signed or create a self-signed certificate. The SSL Certificate status will updated from 'Not FIPS Mode Compliant' to 'FIPS Mode Compliant'.

   When FIPS mode is activated, key files cannot be downloaded or uploaded. The most recently created CSR will be associated internally with the key file. Further, the SSL Certificate from the CA and its private key are not included in the full restore of the backed-up file. The key cannot be exported from KX II.

FIPS 140-2 Support Requirements

The KX II supports the use of FIPS 140-20 approved encryption algorithms. This allows an SSL server and client to successfully negotiate the cipher suite used for the encrypted session when a client is configured for FIPS 140-2 only mode.

Following are the recommendations for using FIPS 140-2 with the KX II:

KX II

- Set the Encryption & Share to Auto on the Security Settings page. See Encryption & Share.

Microsoft Client

- FIPS 140-2 should be enabled on the client computer and in Internet Explorer.

To enable FIPS 140-2 on a Windows client:

1. Select Control Panel > Administrative Tools > Local Security Policy to open the Local Security Settings dialog.
2. From the navigation tree, select Select Local Policies > Security Options.
3. Enable "System Cryptography: Use FIPS compliant algorithms for encryption, hashing and signing".
4. Reboot the client computer.

To enable FIPS 140-2 in Internet Explorer:

1. In Internet Explorer, select Tools > Internet Options and click on the Advanced tab.
2. Select the Use TLS 1.0 checkbox.
3. Restart the browser.

Configuring IP Access Control

Using IP access control, you can control access to your KX II. By setting a global Access Control List (ACL) you are ensuring that your device does not respond to packets being sent from disallowed IP addresses. The IP access control is global, affecting the KX II as a whole, but you can also control access to your device at the group level. See ***Group-Based IP ACL (Access Control List)*** (on page 116) for more information about group-level control.

Important: IP address 127.0.0.1 is used by the KX II local port. When creating an IP Access Control list, 127.0.0.1 should not be within the range of IP addresses that are blocked or you will not have access to the KX II local port.

To use IP access control:

1. Open the IP Access Control page by selecting Security > IP Access Control. The IP Access Control page opens.
2. Select the Enable IP Access Control checkbox to enable IP access control and the remaining fields on the page.
3. Choose the Default Policy. This is the action taken for IP addresses that are not within the ranges you specify.
   - Accept - IP addresses are allowed access to the KX II device.
   - Drop - IP addresses are denied access to the KX II device.

Note: Both IPv4 and IPv6 addresses are supported.

To add (append) rules:

1. Type the IP address and subnet mask in the IPv4/Mask or IPv6/Prefix Length 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 IPv4/Mask or IPv6/Prefix Length 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.

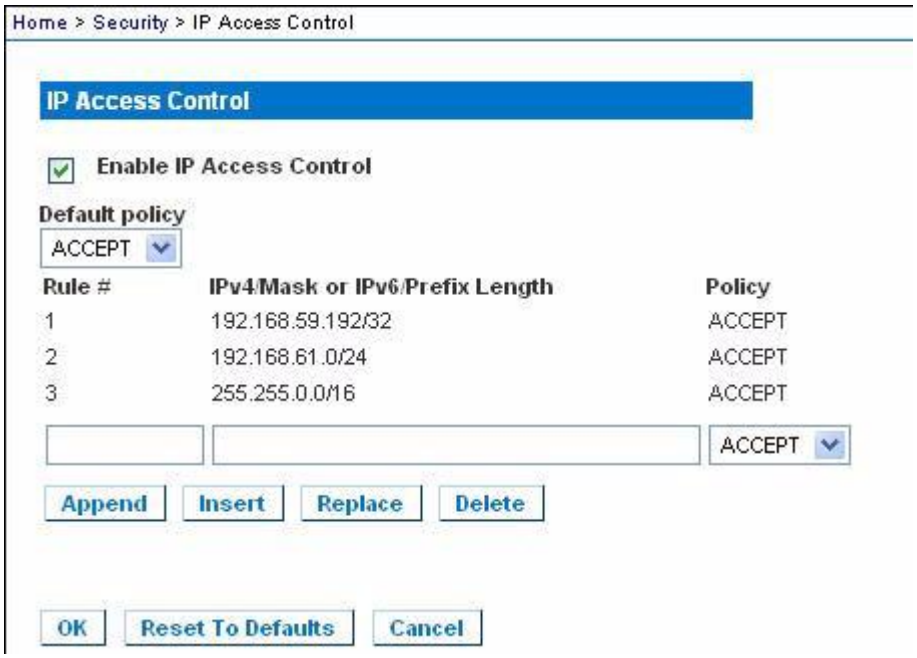
To replace a rule:

1. Specify the rule # you want to replace.
2. Type the IP address and subnet mask in the IPv4/Mask or IPv6/Prefix Length 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.



SSL Certificates

The KX II uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. When establishing a connection, the KX II has to identify itself to a client using a cryptographic certificate.

It is possible to generate a Certificate Signing Request (CSR) and install a certificate signed by the Certificate Authority (CA) on the KX II. The CA verifies the identity of the originator of the CSR. The CA then returns a certificate containing its signature to the originator. The certificate, bearing the signature of the well-known CA, is used to vouch for the identity of the presenter of the certificate.

To create and install a SSL certificate:

1. Select Security > SSL Certificate.
2. Complete the following fields:
   a. Common name - The network name of the KX II once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the KX II with a web browser but without the prefix “http://”. In case the name given here and the actual network name differ, the browser will pop up a security warning when the KX II is accessed using HTTPS.

b. Organizational unit - This field is used for specifying to which department within an organization the KX II belongs.

c. Organization - The name of the organization to which the KX II belongs.

d. Locality/City - The city where the organization is located.

e. State/Province - The state or province where the organization is located.

f. Country (ISO code) - The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the U.S.

g. Challenge Password - Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimum length of this password is four characters.

h. Confirm Challenge Password - Confirmation of the Challenge Password.

i. Email - The email address of a contact person that is responsible for the KX II and its security.

j. Key length - The length of the generated key in bits. 1024 is the default.

k. Select the Create a Self-Signed Certificate checkbox (if applicable).

3. Click Create to generate the Certificate Signing Request (CSR).

To download a CSR certificate:

1. The CSR and the file containing the private key used when generating it can be downloaded by click the Download button.

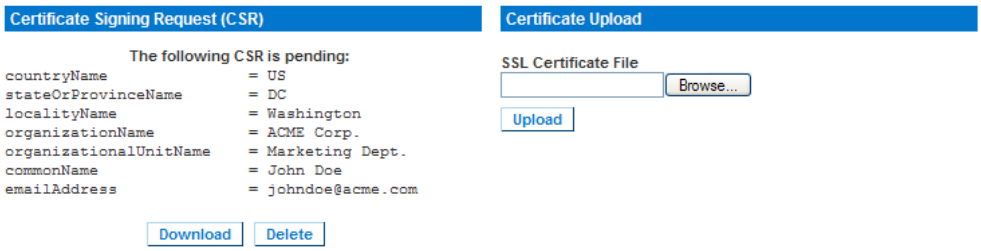
Note: The CSR and the private key file are a matched set and should be treated accordingly. If the signed certificate is not matched with the private key used to generate the original CSR, the certificate will not be useful. This applies to uploading and downloading the CSR and private key files.

2. Send the saved CSR to a CA for certification. You will get the new certificate from the CA.

To upload a CSR:

1. Upload the certificate to the KX II by clicking the Upload button.

Note: The CSR and the private key file are a matched set and should be treated accordingly. If the signed certificate is not matched with the private key used to generate the original CSR, the certificate will not be useful. This applies to uploading and downloading the CSR and private key files.



After completing these three steps the KX II has its own certificate that is used for identifying the card to its clients.

Important: If you destroy the CSR on the KX II there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described above. To avoid this, use the download function so you will have a copy of the CSR and its private key.

Security Banner

KX II provides you with the ability to add a security banner to the KX II login process. This feature requires users to either accept or decline a security agreement before they can access the KX II. The information provided in a security banner will be displayed in a Restricted Service Agreement dialog after users access KX II using their login credentials.

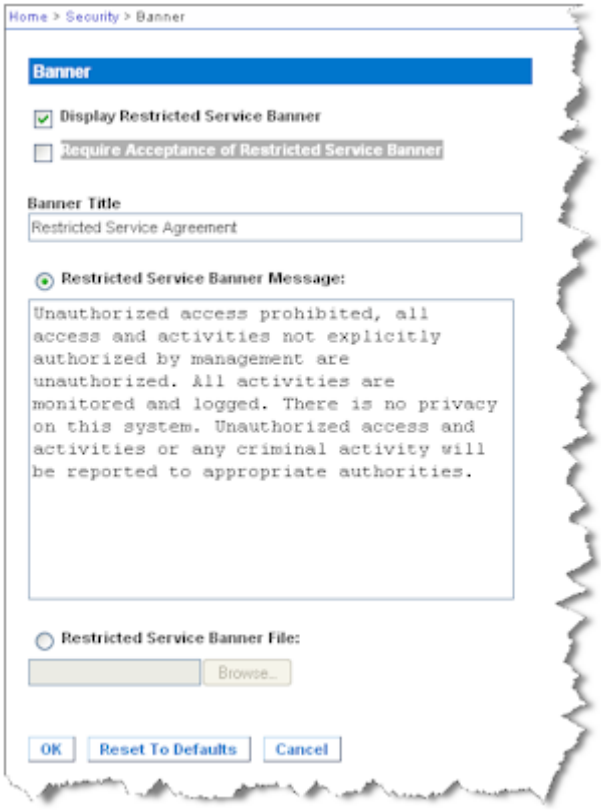
The security banner heading and wording can be customized, or the default text can be used. Additionally, the security banner can be configured to require that a user accepts the security agreement before they are able to access the KX II or it can just be displayed following the login process. If the accept or decline feature is enabled, the user's selection is logged in the audit log.

To configure a security banner:

1. Click Security > Banner to open the Banner page.
2. Select Display Restricted Service Banner to enable the feature.
3. If you want to require users to acknowledge the banner prior to continuing the login process, select Require Acceptance of Restricted Service Banner. In order to acknowledge the banner, users will select a checkbox. If you do not enable this setting, the security banner will only be displayed after the user logs in and will not require users acknowledge it.

4. If needed, change the banner title. This information will be displayed to users as part of the banner. Up to 64 characters can be used.
5. Edit the information in the Restricted Services Banner Message text box. Up to 6000 characters can be entered or uploaded from a text file. To do this, do one of the following:
   a. Edit the text by manually typing in the text box. Click OK.
   b. Upload the information from .txt file by selecting the Restricted Services Banner File radio button and using the Browse feature to locate and upload the file. Click OK. Once the file is uploaded, the text from the file will appear in the Restricted Services Banner Message text box.

Note: You cannot upload a text file from the local port.



Chapter 10 Maintenance

In This Chapter

Audit Log

A log is created of the KX II system events.

To view the audit log for your 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 based on a 24-hour clock.
   - Event - The event name as listed in the Event Management page.
   - Description - Detailed description of the event.

To save the audit log:

Note: Saving the audit log is available only on the KX II Remote Console, not on the Local Console.

1. Click Save to File. 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 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 KX II and CIMs:

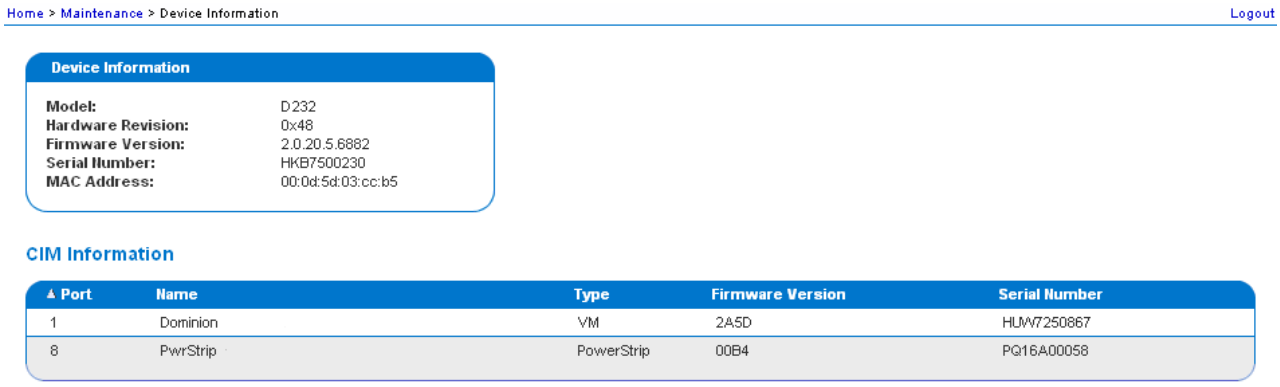
- Choose Maintenance > Device Information. The Device Information page opens.

The following information is provided about the 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, Rack PDU, or VM
- Firmware Version
- Serial Number



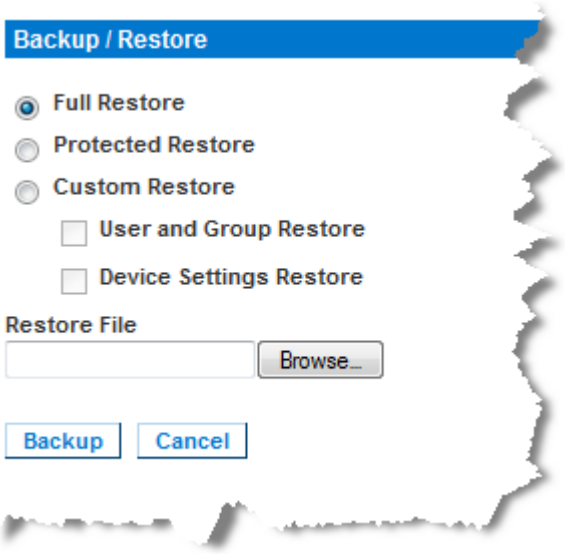
Backup and Restore

From the Backup/Restore page, you can backup and restore the settings and configuration for your 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 KX II by backing up the user configuration settings from the KX II in use and restoring those configurations to the new KX II. You can also set up one KX II and copy its configuration to multiple 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.

If you are using Firefox® or Internet Explorer® 5 or lower, to backup your 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.

If you are using Internet Explorer 6 or higher, to backup your KX II:

1. Click Backup. A File Download dialog appears that contains an Open button. Do not click Open.

   In IE 6 and higher, IE is used as the default application to open files, so you are prompted to open the file versus save the file. To avoid this, you must change the default application that is used to open files to WordPad®.

2. To do this:

   a. Save the backup file. The backup file is saved locally on your client machine with the name and location specified.

   b. Once saved, locate the file and right-click on it. Select properties.

   c. In general tab, click Change and select WordPad.

To restore your KX II:

WARNING: Exercise caution when restoring your 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 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 IP address, name, and so forth. With this option, you can setup one KX II and copy the configuration to multiple KX II devices.
- Custom Restore - With this option, you can select User and Group Restore, Device Settings Restore, or both:
  - User and Group Restore - This option includes only user and group information. This option *does not* restore the certificate and the private key files. Use this option to quickly set up users on a different KX II.
  - Device Settings Restore - This option includes only device settings such as power associations, USB profiles, blade chassis related configuration parameters, and Port Group assignments. Use this option to quickly copy the device information.

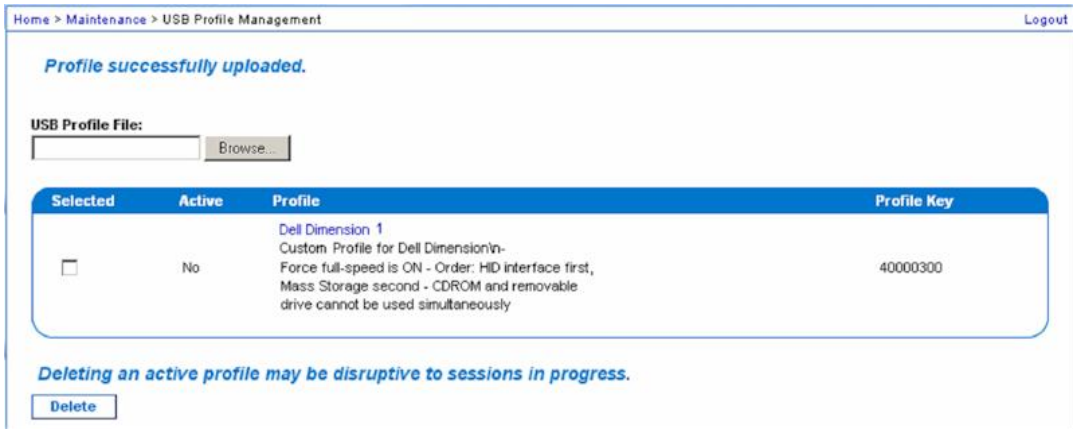
1. Click Browse. A Choose File dialog appears.
2. Navigate to and select the appropriate backup file and click Open. The selected file is listed in the Restore File field.
3. Click Restore. The configuration (based on the type of restore selected) is restored.

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.



To upload a custom profile to your 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 continue with the upload by clicking Upload or cancel it by clicking on Cancel.

To delete a custom profile to your 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 216) for more information.

Upgrading CIMs

Use this procedure to upgrade CIMs using the firmware versions stored in the memory of your KX II device. 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 D2CIM-VUSB or D2CIM-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 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

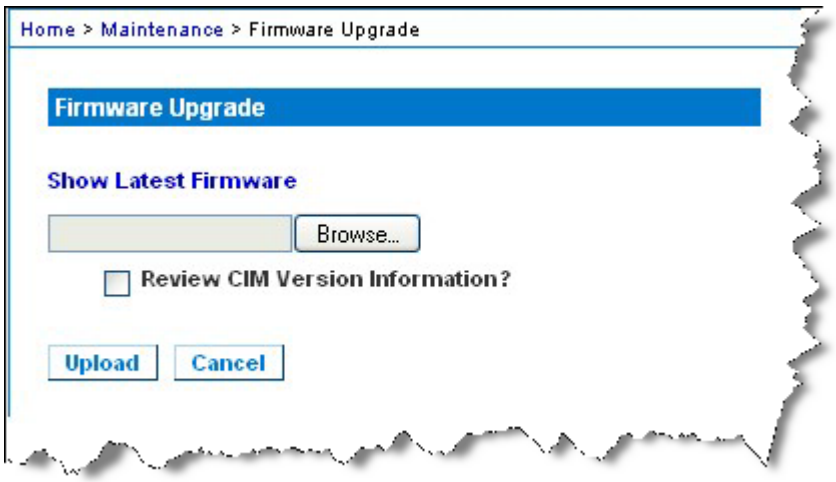
Use the Firmware Upgrade page to upgrade the firmware for your KX II and all attached CIMs. This page is available in the KX II Remote Console only.

Important: Do not turn off your 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 KX II unit:

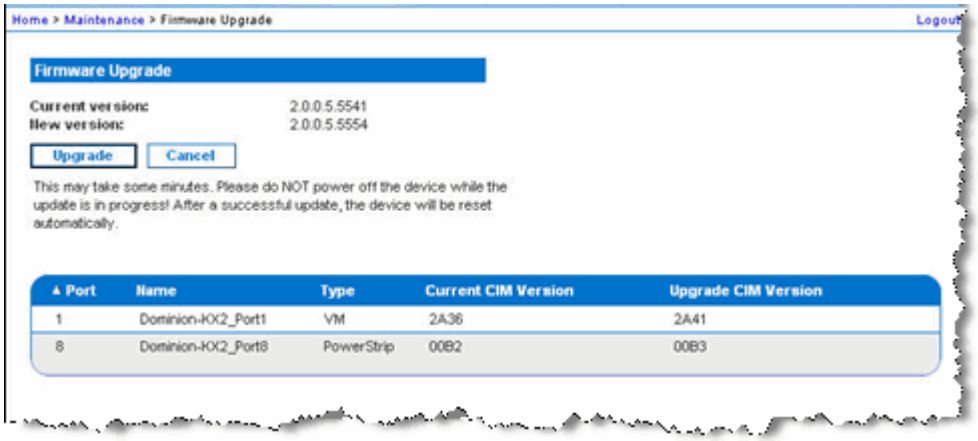
1. Locate the appropriate Raritan firmware distribution file (*.RFP) on the ***Raritan website http://www.raritan.com*** on the Firmware Upgrades web page.
2. Unzip the file. Please read all instructions included in the firmware ZIP files carefully before upgrading.

   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.



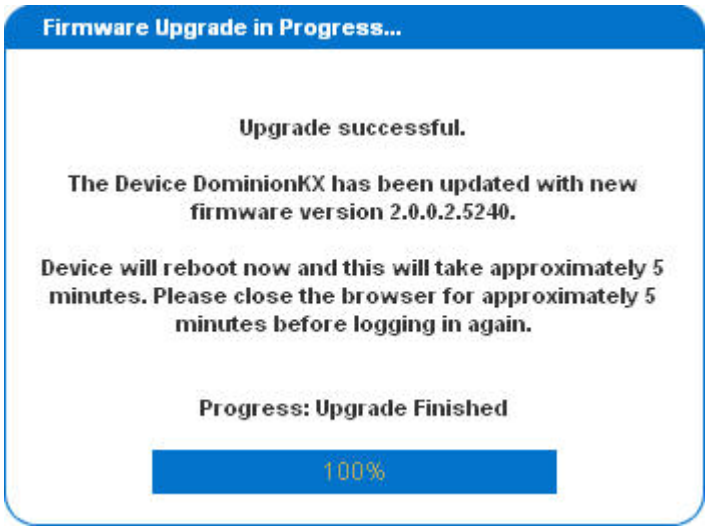
4. Click the Browse button to navigate to the directory where you unzipped the upgrade file.
5. Select the Review CIM Version Information? checkbox if you would like information displayed about the versions of the CIMs in use.

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):



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).



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

For information about upgrading the device firmware using the Multi-Platform Client, see Upgrading Device Firmware in the **KVM and Serial Access Clients Guide**.

Note: Firmware upgrades are not supported via modem.

Note: If you are using a tiered configuration in which a base KX II device is used to access multiple other tiered devices, you may receive a low memory error during a firmware upgrade if you have a large number of user groups. If you receive this error, reboot the device and then perform the upgrade again. If you continue to receive this error after rebooting, disable tiering on the base device and perform the upgrade again.

Upgrade History

The KX II provides information about upgrades performed on the KX II and attached CIMS.

To view the upgrade history:

- Choose Maintenance > Upgrade History. The Upgrade History page opens.

Information is provided about the 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:

- Type - The type of CIM.
- Port - The port where the CIM is connected.
- User - The user who performed the upgrade.
- IP - IP address firmware location.
- Start Time - Start time of the upgrade.
- End Time - end time of the upgrade.
- Previous Version - Previous CIM firmware version.
- Upgrade Version - Current CIM firmware version.
- CIMs - Upgraded CIMs.
- Result - The result of the upgrade (success or fail).

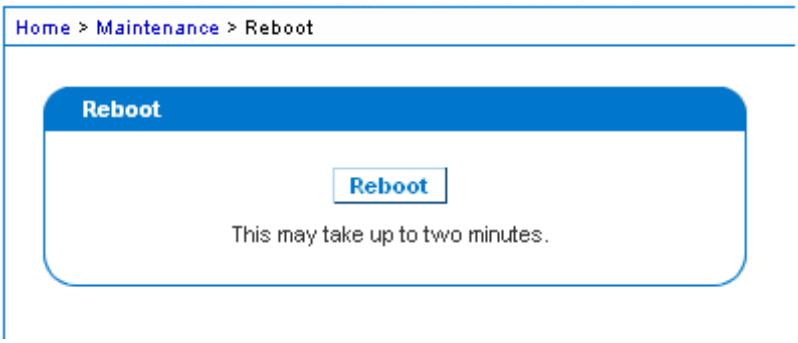
Rebooting

The Reboot page provides a safe and controlled way to reboot your KX II. This is the recommended method for rebooting.

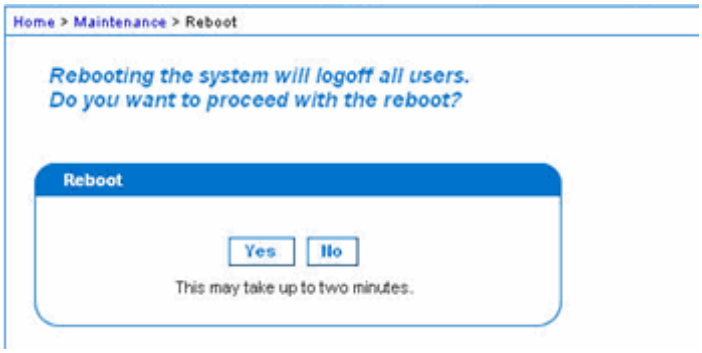
Important: All KVM and serial connections will be closed and all users will be logged off.

To reboot your KX II:

1. Choose Maintenance > Reboot. The Reboot page opens.



2. Click Reboot. You are prompted to confirm the action. Click Yes to proceed with the reboot.



Stopping CC-SG Management

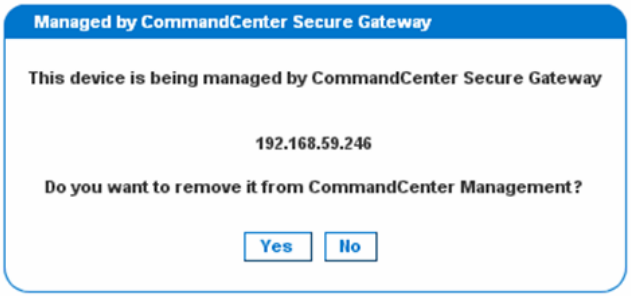
While the KX II is under CC-SG management, if you try to access the device directly, you are notified that it the device is under CC-SG management.

If you are managing the KX II through CC-SG and connectivity between CC-SG and the KX II is lost after the specified timeout interval (typically 10 minutes), you are able to end the CC-SG management session from the KX II console.

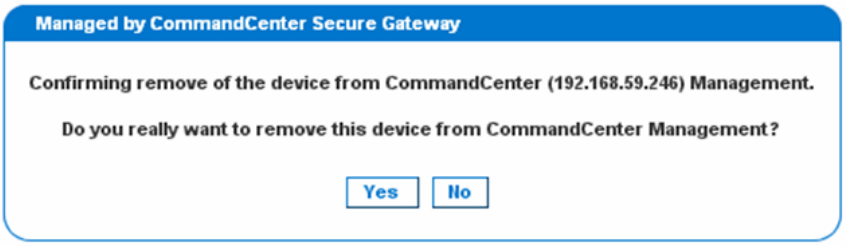
Note: You must have the appropriate permissions to end CC-SG management of the KX II. Additionally, the Stop CC-SG Management option will not be provided unless you are currently using CC-SG to manage the KX II.

To stop CC-SG management of a KX II:

1. Click Maintenance > Stop CC-SG Management. A message indicating that the device is being managed by CC-SG will be displayed. An option to remove the device from CC-SG management will also be displayed.



2. Click Yes to begin the processing of removing the device from CC-SG management. A confirmation message will then displayed asking you to confirm that you want the remove the device from CC-SG management.



3. Click Yes to remove the device CC-SG management. Once CC-SG management has ended, a confirmation will be displayed.

Chapter 11 Diagnostics

In This Chapter

Network Interface Page

The KX II provides information about the status of your network interface.

To view information about your network interface:

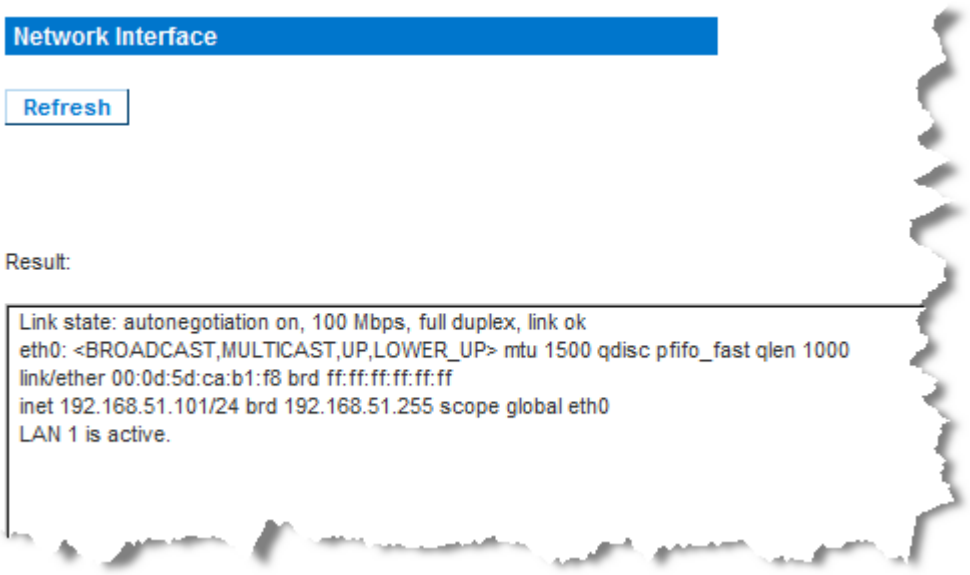
- Choose Diagnostics > Network Interface. The Network Interface page opens.

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.

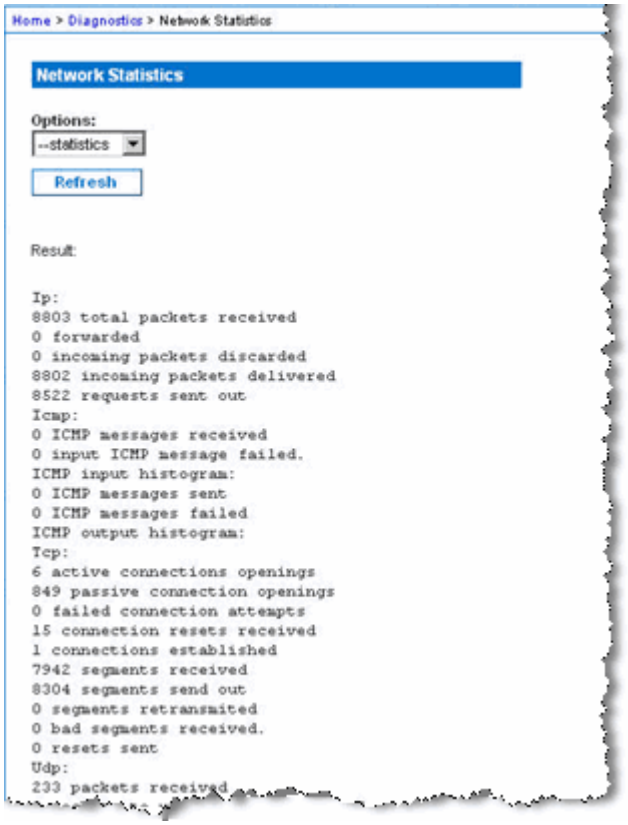


Network Statistics Page

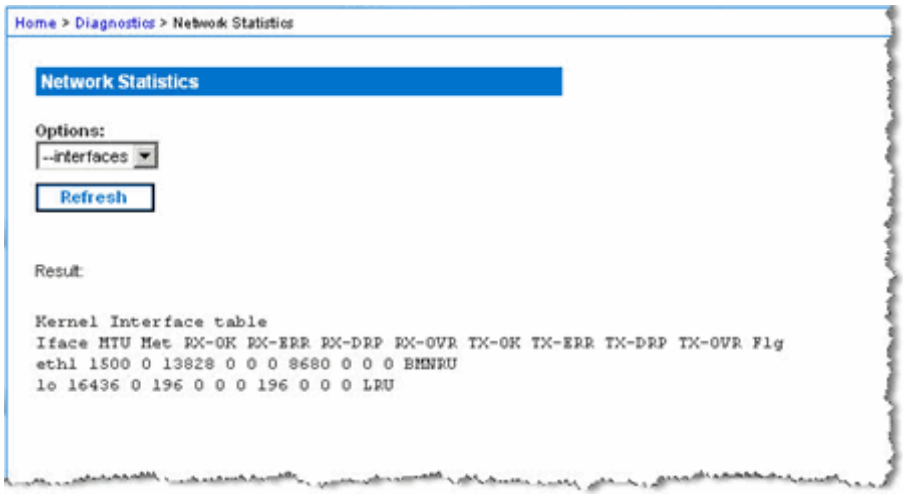
The KX II provides statistics about your network interface.

To view statistics about your network interface:

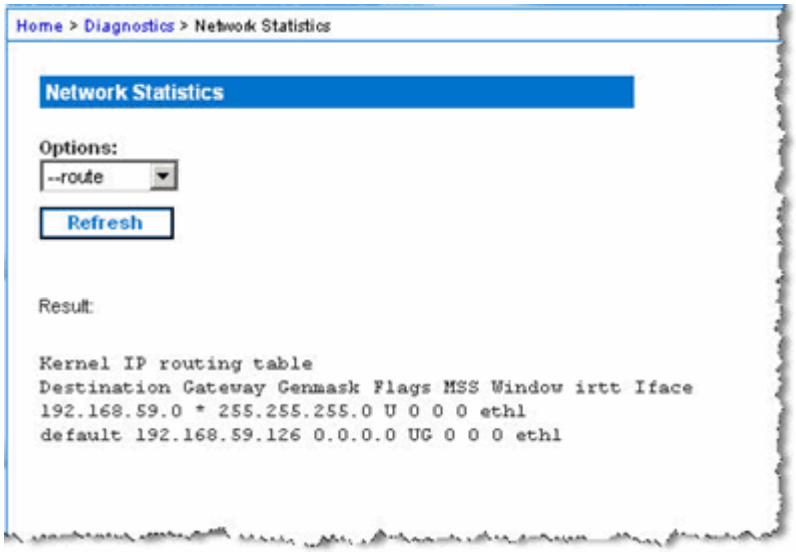
1. Choose Diagnostics > Network Statistics. The Network Statistics page opens.
2. Choose the appropriate option from the Options drop-down list:
   - Statistics - Produces a page similar to the one displayed here.



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



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



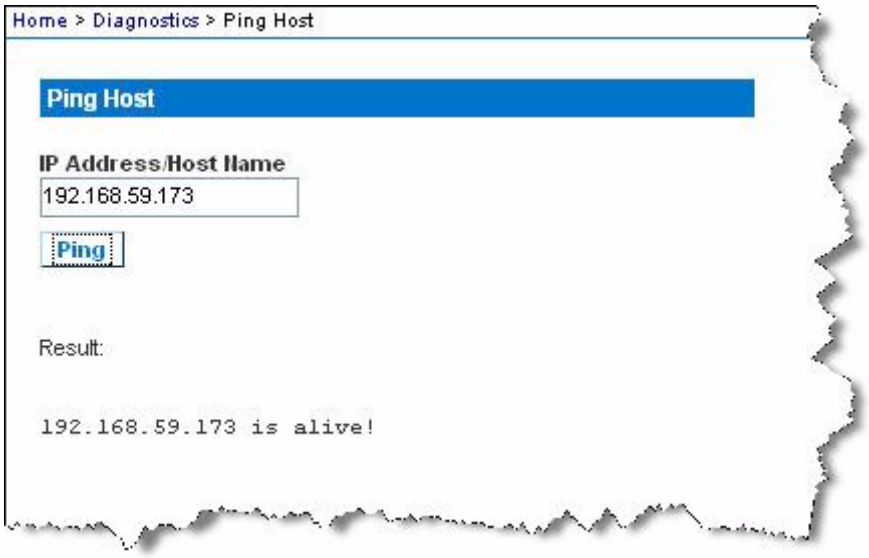
3. Click Refresh. The relevant information is displayed in the Result field.

Ping Host Page

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

To ping the host:

1. Choose Diagnostics > Ping Host. The Ping Host page appears.



2. Type either the hostname or IP address into the IP Address/Host Name field.

Note: The host name cannot exceed 232 characters in length.

3. Click Ping. The results of the ping are displayed in the Result field.

Note: Both IPv4 and IPv6 addresses are supported.

Trace Route to Host Page

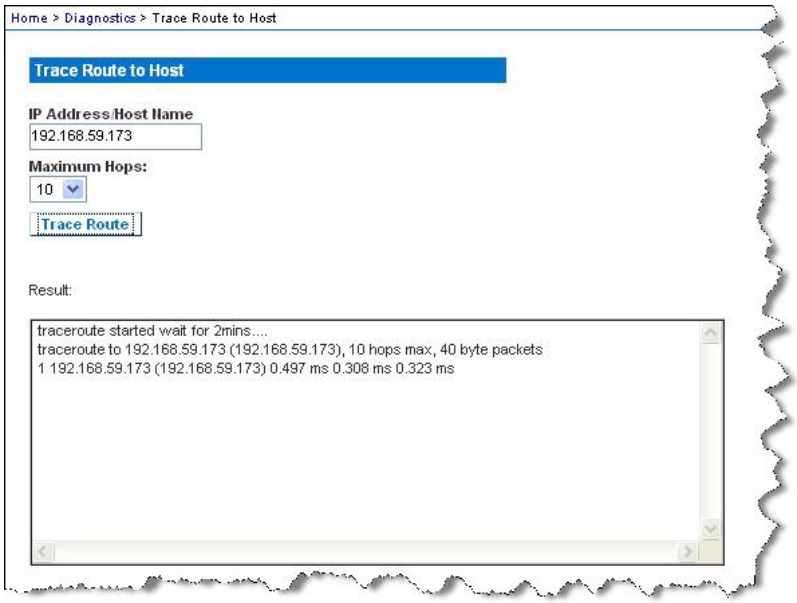
Trace route is a network tool used to determine the route taken to the provided hostname or IP address.

To trace the route to the host:

1. Choose Diagnostics > Trace Route to Host. The Trace Route to Host page opens.
2. Type either the IP address or host name into the IP Address/Host Name field.

Note: The host name cannot exceed 232 characters in length.

3. Choose the maximum hops from the drop-down list (5 to 50 in increments of 5).
4. Click Trace Route. 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.

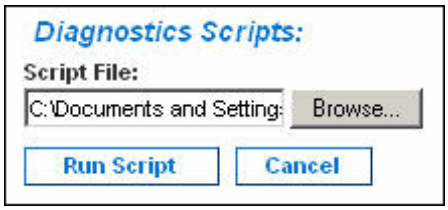
Device diagnostics downloads the diagnostics information from the KX II to the client machine. Two operations can be performed on this page:

- Execute a special diagnostics script provided by Raritan Technical Support during a critical error debugging session. The script is uploaded to the device 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 KX II device to the client. This encrypted file is then sent to Raritan Technical Support. Only Raritan can interpret this file.

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

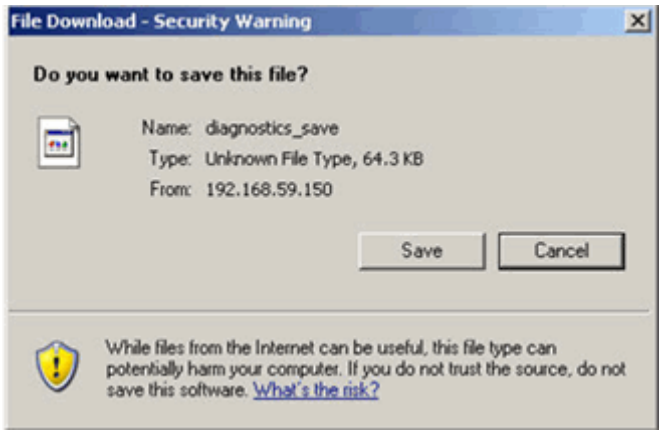
To run the KX II System diagnostics:

1. Choose Diagnostics > KX II Diagnostics. The 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.



   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.



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.

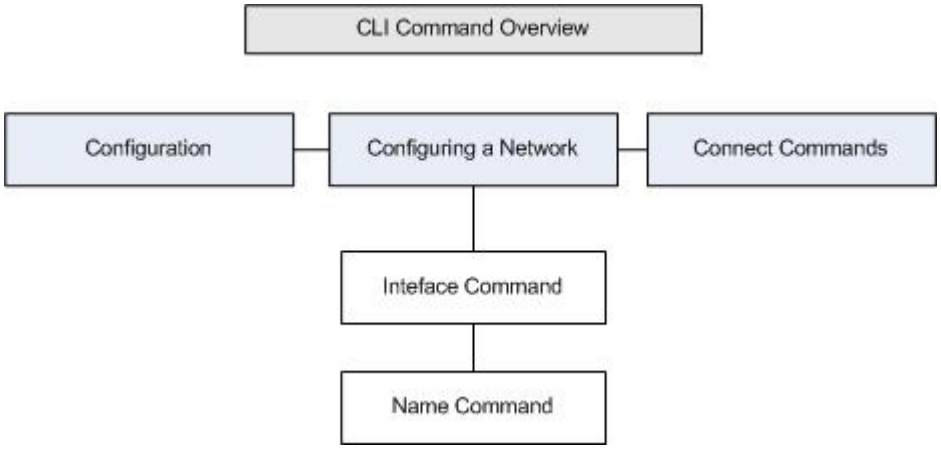
Chapter 12 Command Line Interface (CLI)

In This Chapter

Overview

The Command Line Interface(CLI) can be used to configure the KX II network interface and perform diagnostic functions provided you have the appropriate permissions to do so.

The following figures describe an overview of the CLI commands. See ***CLI Commands*** (on page 238) for a list of all the commands, which include definitions and links to the sections in this chapter that give examples of these commands.



The following common commands can be used from all levels of the CLI to the preceding figure: top, history, log off, quit, show, and help.

Note: Both IPv4 and IPv6 addresses are supported.

Accessing the KX II Using CLI

Access the KX II by using one of the following methods:

- SSH (Secure Shell) via IP connection

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

- Putty - ***http://www.chiark.greenend.org.uk/~sgtatham/putty/ http://www.chiark.greenend.org.uk/~sgtatham/putty/***
- SSH Client from ssh.com - ***www.ssh.com http://www.ssh.com***
- Applet SSH Client - ***www.netspace.org/ssh http://www.netspace.org/ssh***
- OpenSSH Client - ***www.openssh.org http://www.openssh.org***

SSH Connection to the KX II

Use any SSH client that supports SSHv2 to connect to the KX II. You must enable SSH access from the Devices Services page.

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

SSH Access from a Windows PC

To open an SSH session from a Windows® PC:

1. Launch the SSH client software.
2. Enter the IP address of the KX II server. For example, 192.168.0.192.
3. Choose SSH, which uses the default configuration port 22.
4. Click Open.

The `login as:` prompt appears.

See ***Logging In*** (on page 234).

Note: Both IPv4 and IPv6 addresses are supported.

SSH Access from a UNIX/Linux Workstation

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

```
ssh -l admin 192.168.30.222
```

The Password prompt appears.

See ***Logging In*** (on page 234).

Note: Both IPv4 and IPv6 addresses are supported.

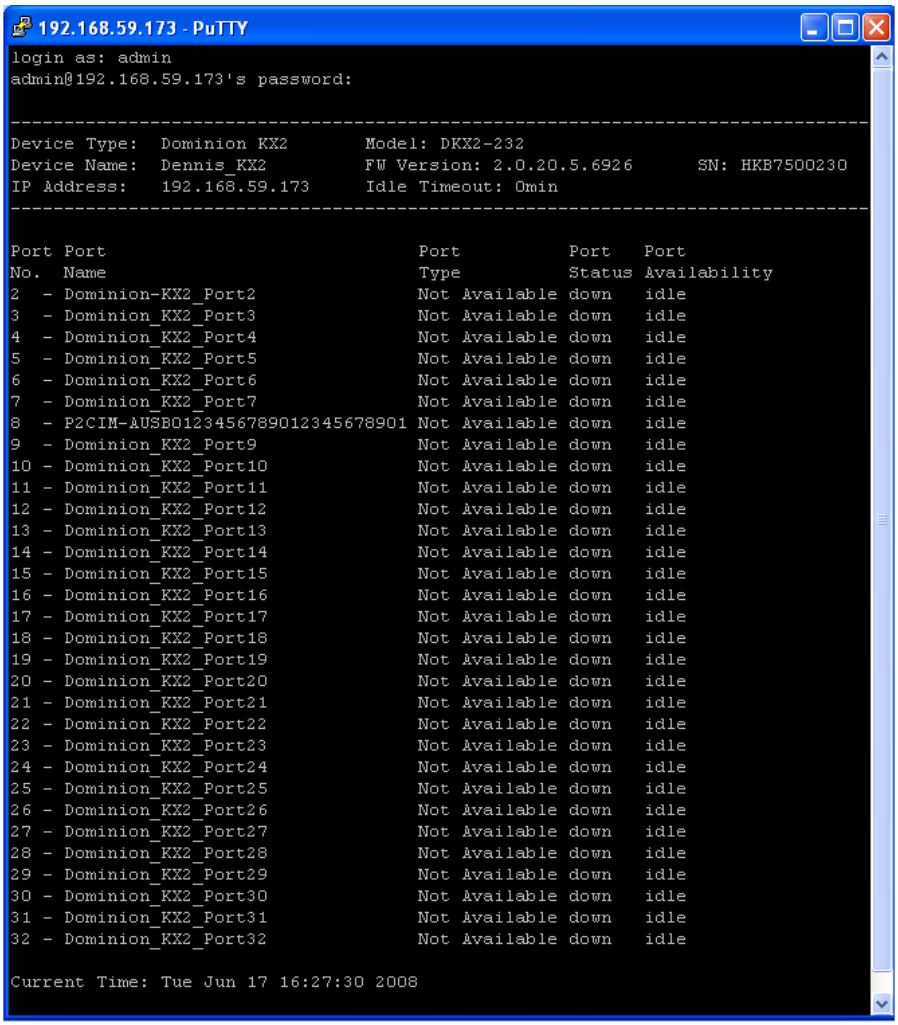
Logging In

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

1. Log in as `admin`
2. The Password prompt appears. Enter the default password: *raritan*

   The welcome message displays. You are now logged on as an administrator.

After reviewing the following ***Navigation of the CLI*** (on page 235) section, perform the Initial Configuration tasks.



Navigation of the CLI

Before using the CLI, it is important to understand CLI navigation and syntax. There are also some keystroke combinations that simplify CLI use.

Completion of Commands

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

- If no match is found, the CLI displays the valid entries for that level.
- If multiple matches are found, the CLI displays all valid entries.

Enter additional text to make the entry unique and press the Tab key to complete the entry.

CLI Syntax -Tips and Shortcuts

Tips

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

Shortcuts

- Press the Up arrow key to display the last entry.
- Press Backspace to delete the last character typed.
- Press Ctrl + C to terminate a command or cancel a command if you typed the wrong parameters.
- Press Enter to execute the command.
- Press Tab to complete a command. For example, `Admin Port > Conf.` The system then displays the `Admin Port > Config >` prompt.

Common Commands for All Command Line Interface Levels

Following are the commands that are available at all CLI levels. These commands also help navigate through the CLI.

Commands	Description
top	Return to the top level of the CLI hierarchy, or the “username” prompt.
history	Display the last 200 commands the user entered into the KX II CLI.

Commands	Description
help	Display an overview of the CLI syntax.
quit	Places the user back one level.
logout	Logs out the user session.

Initial Configuration Using CLI

Note: These steps, which use the CLI, are optional since the same configuration can be done via KVM. See **Getting Started** *(on page 14) for more information.*

KX II devices come from the factory with default factory settings. When you first power up and connect to the device, you must set the following basic parameters so the device can be accessed securely from the network:

1. Reset the administrator password. All KX II devices are shipped with the same default password. Therefore, to avoid security breaches it is imperative that you change the admin password from raritan to one customized for the administrators who will manage the KX II device.
2. Assign the IP address, subnet mask, and gateway IP address to allow remote access.

Note: Both IPv4 and IPv6 addresses are supported.

Setting Parameters

To set parameters, you must be logged on with administrative privileges. At the top level, you will see the `"Username" >` prompt, which for the initial configuration is `"admin"`. Enter the top command to return to the top menu level.

Note: If you have logged on with a different user name, that user name will appear instead of admin.

Setting Network Parameters

Network parameters are configured using the interface command.

```
admin > Config > Network > interface ipauto none ip
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1 mode
auto
```

When the command is accepted, the device automatically drops the connection. You must reconnect to the device using the new IP address and the user name and password you created in the resetting factory default password section.

Important: If the password is forgotten, the KX II will need to be reset to the factory default from the Reset button on the back of the KX II. The initial configuration tasks will need to be performed again if this is done.

The KX II now has the basic configuration and can be accessed remotely via SSH, GUI, or locally using the local serial port. The administrator needs to configure the users and groups, services, security, and serial ports to which the serial targets are attached to the KX II.

Note: Both IPv4 and IPv6 addresses are supported.

CLI Prompts

The Command Line Interface prompt indicates the current command level. The root portion of the prompt is the login name. For a direct admin serial port connection with a terminal emulation application, Admin Port is the root portion of a command.

```
admin >
```

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

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

0

CLI Commands

- Enter `admin > help`.

Command	Description
config	Change to config sub menu.
diagnostics	Change to diag sub menu.
help	Display overview of commands.

Command	Description
history	Display the current session's command line history.
listports	List accessible ports.
logout	Logout of the current CLI session.
top	Return to the root menu.
userlist	List active user sessions.

- Enter `admin > config > network`.

Command	Description
help	Display overview of commands.
history	Display the current session's command line history.
interface	Set/get network parameters.
ipv6_interface	Set/get IPv6 network parameters.
logout	Logout of the current CLI session.
name	Device name configuration.
quit	Return to previous menu.
stop	Return to the root menu.

Security Issues

Elements to consider when addressing security for console servers:

- Encrypting the data traffic sent between the operator console and the KX II device.
- Providing authentication and authorization for users.
- Security profile.

The KX II supports each of these elements; however, they must be configured prior to general use.

Administering the KX II Console Server Configuration Commands

Note: CLI commands are the same for SSH and Local Port access sessions.

The Network command can be accessed in the Configuration menu for the KX II.

Configuring Network

The network menu commands are used to configure the KX II network adapter.

Commands	Description
interface	Configure the KX II device network interface.
name	Network name configuration
ipv6	Set/get IPv6 network parameters.

Interface Command

The Interface command is used to configure the KX II network interface. The syntax of the interface command is:

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask
<subnetmask>] [gw <ipaddress>] [mode <mode>]

Set/Get ethernet parameters

ipauto <none|dhcp> IP auto configuration (none/dhcp)

ip <ipaddress> IP Address

mask <subnetmask> Subnet Mask

gw <ipaddress> Gateway IP Address

mode <mode> Set Ehternet Mode
(auto/10hdx/10fdx/100hdx/100fdx/1000fdx)
```

Interface Command Example

The following command enables the interface number 1, sets the IP address, mask, and gateway addresses, and sets the mode to auto detect.

```
Admin > Config > Network > interface ipauto none ip
192.16.151.12 mask 255.255.255.0 gw 192.168.51.12 mode
auto
```

Note: Both IPv4 and IPv6 addresses are supported.

Name Command

The name command is used to configure the network name. The syntax of the name is:

```
name [devicename <devicename>] [hostname <hostname>]
```

Device name configuration

```
devicename <devicename>   Device Name

hostname   <hostname>     Preferred host name (DHCP
only)
```

Name Command Example

The following command sets the network name:

```
Admin > Config > Network > name devicename My-KSX2
```

IPv6 Command

Use the IPv6_command to set IPv6 network parameters and retrieve existing IPv6 parameters.

Chapter 13 KX II Local Console

In This Chapter

Overview

The 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 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 KX II Local Console provides the same administrative functionality as the KX II Remote Console.

Using the KX II Local Console

Simultaneous Users

The 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 KX II, you can still simultaneously access your servers from the rack via the Local Console.

KX II Local Console Interface

When you are located at the server rack, the KX II provides standard KVM management and administration via the KX II Local Console. The 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. Additionally, the KX II provides terminal emulation when accessing serial targets.

There are many similarities among the KX II Local Console and the KX II Remote Console graphical user interfaces. Where there are differences, they are noted in the help.

The KX II Local Console Factory Reset option is available in the KX II Local Console but not the KX II Remote Console.

Security and Authentication

In order to use the KX II Local Console, you must first authenticate with a valid username and password. The KX II provides a fully-integrated authentication and security scheme, whether your access is via the network or the local port. In either case, the KX II allows access only to those servers to which a user has access permissions. See ***User Management*** (on page 110) for additional information on specifying server access and security settings.

If your 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 KX II Local Console:

1. Connect a keyboard, mouse, and video display to the local ports at the back of the KX II.
2. Start the KX II. The KX II Local Console interface displays.

Local Console Smart Card Access

To use a smart card to access a server at the Local Console, plug a USB smart card reader into the KX II using one of the USB ports located on the KX II. Once a smart card reader is plugged in or unplugged from the KX II, the KX II autodetects it. For a list of supported smart cards and additional system requirements, see ***Supported and Unsupported Smart Card Readers*** (on page 275) and ***Minimum System Requirements*** (on page 276).

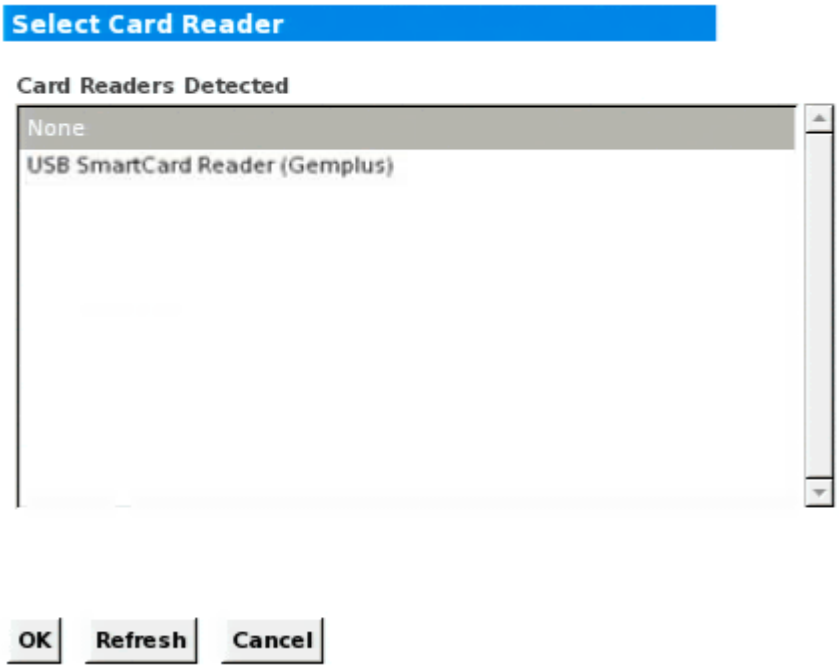
When mounted onto the target server, the card reader and smart card will cause the server to behave as if they had been directly attached. Removal of the smart card or smart card reader will cause the user session to be locked or you will be logged out depending on how the card removal policy has been setup on the target server OS. When the KVM session is terminated, either because it has been closed or because you switch to a new target, the smart card reader will be automatically unmounted from the target server.

To mount a smart card reader onto a target via the KX II Local console:

1. Plug a USB smart card reader into the KX II using one of the USB ports located on the device. Once attached, the smart card reader will be detected by the KX II.
2. From the Local Console, click Tools.
3. Select the smart card reader from the Card Readers Detected list. Select None from the list if you do not want a smart card reader mounted.
4. Click OK. Once the smart card reader is added, a message will appear on the page indicating you have completed the operation successfully. A status of either Selected or Not Selected will appear in the left panel of the page under Card Reader.

To update the Card Readers Detected list:

- Click Refresh if a new smart card has been mounted. The Card Readers Detected list will be refreshed to reflect the newly added smart card reader.



Smart Card Access in KX2 8 Devices

If you are using a smart card reader to access a server from the Local Console through a KX2-832 or KX2-864 device, the extended local port (Local Port Settings page) must be disabled. The extended local port does not support smart card authentication.

Local Console USB Profile Options

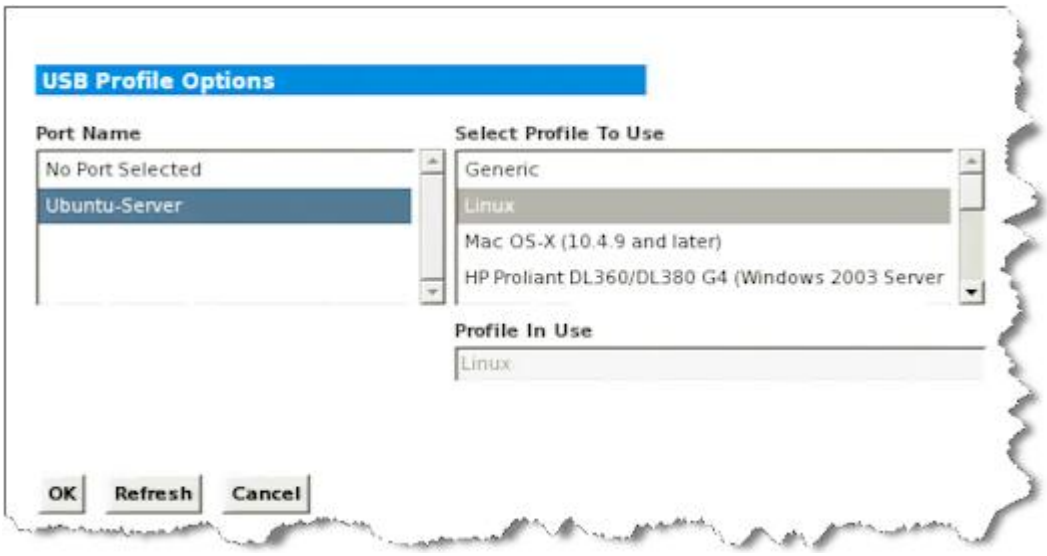
From the USB Profile Options section of the Tools page, you can choose from the available USB profiles for a local port.

The ports that can be assigned profiles are displayed in the Port Name field and the profiles that are available for a port appear in the Select Profile To Use field after the port is selected. The profiles selected for use with a port appear in the Profile In Use field.

To apply a USB profile to a local console port:

1. In the Port Name field, select the port you want to apply the USB profile to.

2. In the Select Profile To Use field, select the profile to use from among those available for the port.
3. Click OK. The USB profile will be applied to the local port and will appear in the Profile In Use field.



Available Resolutions

The 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.

Port Access Page (Local Console Server Display)

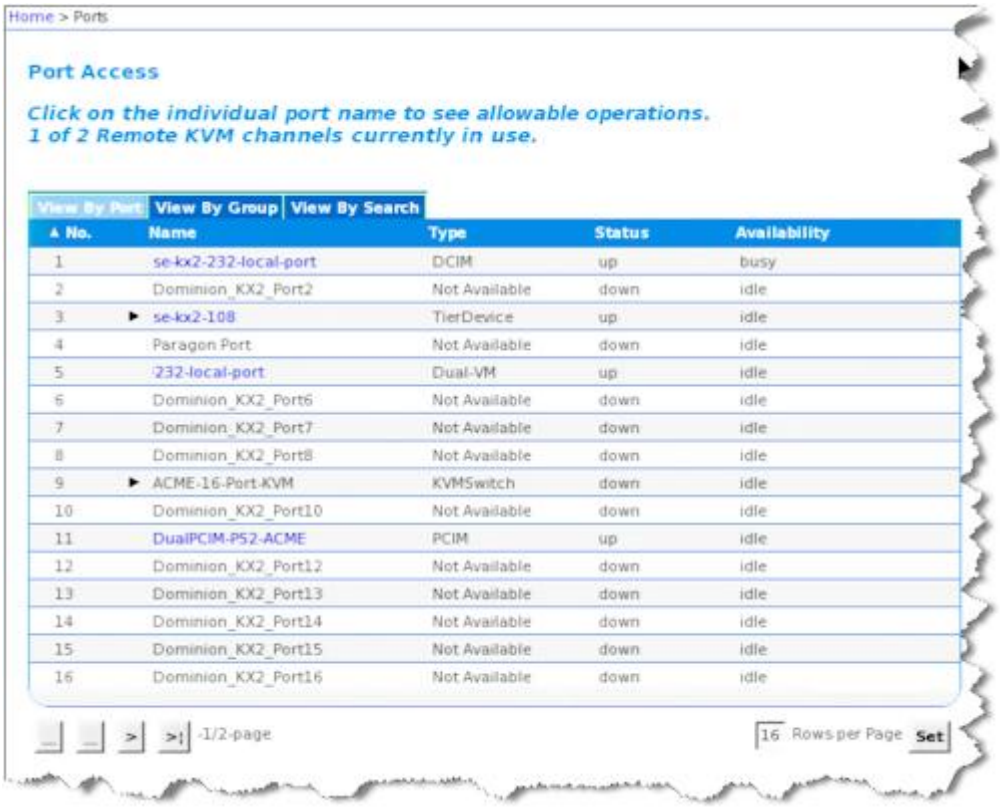
After you login to the KX II Local Console, the Port Access page opens. This page lists all of the KX II ports, the connected KVM target servers, and their status and availability.

Also displayed on the Port Access page are blade chassis that have been configured in the KX II. The blade chassis is displayed in an expandable, hierarchical list on the Port Access page, with the blade chassis at the root of the hierarchy and the individual blades labeled and displayed below the root. Use the Expand Arrow icon next to the root chassis to display the individual blades.

Note: To view the blade chassis in a hierarchal order, blade-chassis subtypes must be configured for the blade server chassis.

If you are using a tiered configuration in which a base KX II device is used to access multiple other tiered devices, the tiered devices are viewed on the Port Access page by clicking on the Expand Arrow icon ▶ to the left of the base device name. See ***Configuring and Enabling Tiering*** (on page 142) for more information on tiering.

By default, the View by Port tab will be displayed on the Port Access page. The View by Group tab displays port groups and can be expandable to display ports that are assigned to the port group. The View by Search tab allows you to search by port name. The search feature supports the use of an asterisk (*) as a wildcard, and full and partial names.



To use the Port Access page:

1. Log in to the Local Console.

   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 KX II device. 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 KX II port. Initially, this is 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 appears.

   Note: Do not use apostrophes for the Port (CIM) Name.

   - Status - The status for standard servers is either up or down.
   - Type - The type of server or CIM. For blade chassis, the type can be Blade Chassis, Blade, BladeChassisAdmin, and BladeChassisURL. Type also includes TierDevice and KVMSwitch.

2. Click View by Port or View by Group to switch between views.
   - In addition to the Port Number, Port Name, Status, Type, and Availability, a Group column is also displayed on the View by Group tab. This column contains the port groups that are available.
3. Click the Port Name of the target server you want to access. The Port Action Menu appears. See **Port Action Menu** (on page 44) for details on available menu options.
4. Choose the desired menu command from the Port Action Menu.

To change the display sort order:

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

Hot Keys and Connect Keys

Because the KX II Local Console interface is completely replaced by the interface for the target server you are accessing, a hot key is used to disconnect from a target and return to the local port GUI. A connect key is used to connect to a target or switch between targets.

The Local Port hot key allows you to rapidly access the 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. See KX II Local Console Local Port Settings for more information.

Connect Key Examples

Standard servers	
Connect key action	**Key sequence example**
Access a port from the local port GUI	Access port 5 from the local port GUI: • Press Left ALT > Press and Release 5 > Release Left ALT
Switch between ports	Switch from target port 5 to port 11: • Press Left ALT > Press and Release 1 > Press and Release 1 > Release Left ALT
Disconnect from a target and return to the local port GUI	Disconnect from target port 11 and return to the local port GUI (the page from which you connected to target): • Double Click Scroll Lock

Blade chassis Connect key action	Key sequence example
Access a port from the local port GUI	Access port 5, slot 2: • Press Left ALT > Press and Release 5 > Press and Release - > Press and Release 2 > Release Left ALT
Switch between ports	Switch from target port 5, slot 2 to port 5, slot 11: • Press Left ALT > Press and Release 5 > Press and Release - > Press and Release 1 > Press and Release 1 > Release Left ALT
Disconnect from a target and return to the local port GUI	Disconnect from target port 5, slot 11 and return to the local port GUI (the page from which you connected to target): • Double Click Scroll Lock

Special Sun Key Combinations

The following key combinations for Sun™ Microsystems server's special keys operate on the local port. These special are available from the Keyboard menu when you connect to a Sun target server:

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

Sun key	Local port key combination
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	No key combination
Power	No key combination

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. The video display switches to the target server interface.

Returning to the KX II Local Console Interface

Important: The 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 KX II Local Console Local Port Settings.

To return to the 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 KX II Local Console interface.

Local Port Administration

The KX II can be managed by either the KX II Local Console or the KX II Remote Console. Note that the KX II Local Console also provides access to:

- Factory Reset
- Local Port Settings(available in the Remote Console, as well)

Note: Only users with administrative privileges can access these functions.

Configuring KX II Local Console Local Port Settings

From the Local Port Settings page, you can customize many settings for the KX II Local Console including keyboard, hot keys, video switching delay, power save mode, local user interface resolution settings, and local user authentication.

Note: Only users with administrative privileges can access these functions.

To configure the local port settings:

Note: Some changes you make to the settings on the Local Port Settings page will restart the browser you are working in. If a browser restart will occur when a setting is changed, it is noted in the steps provider here.

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. The browser will be restarted when this change is made.
   - US
   - US/International
   - United Kingdom
   - French (France)
   - German (Germany)
   - JIS (Japanese Industry Standard)
   - Simplified Chinese
   - Traditional Chinese
   - Dubeolsik Hangul (Korean)
   - German (Switzerland)
   - Portuguese (Portugal)
   - Norwegian (Norway)
   - Swedish (Sweden)
   - Danish (Denmark)
   - Belgian (Belgium)

   Note: Keyboard use for Chinese, Japanese, and Korean is for display only. Local language input is not supported at this time for KX II Local Console functions.

3. Choose the local port hotkey. The local port hotkey is used to return to the 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:

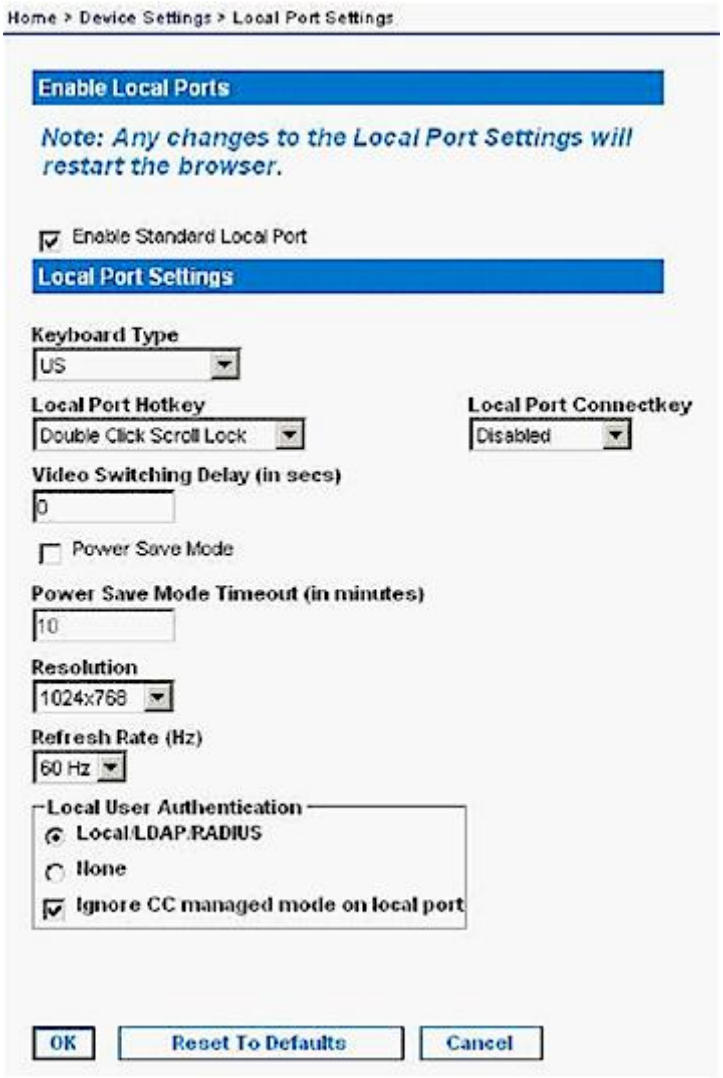
Hot key:	Take this action:
Double Click Scroll Lock	Press Scroll Lock key twice quickly
Double Click Num Lock	Press Num Lock key twice quickly
Double Click Caps Lock	Press Caps Lock key twice quickly
Double Click Left Alt key	Press the left Alt key twice quickly
Double Click Left Shift key	Press the left Shift key twice quickly
Double Click Left Ctrl key	Press the left Ctrl key twice quickly

4. Select the Local Port Connect key. Use a connect key sequence to connect to a target and switch to another target. You can then use the hot key to disconnect from the target and return to the local port GUI. The connect key works for both standard servers and blade chassis. Once the local port connect key is created, it will appear in the Navigation panel of the GUI so you can use it as a reference. See ***Connect Key Examples*** (on page 249) for examples of connect key sequences.
5. 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).
6. 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.
7. Choose the resolution for the KX II Local Console from the drop-down list. The browser will be restarted when this change is made.
   - 800x600
   - 1024x768
   - 1280x1024
8. Choose the refresh rate from the drop-down list. The browser will be restarted when this change is made.
   - 60 Hz
   - 75 Hz
9. Choose the type of local user authentication.
   - Local/LDAP/RADIUS. This is the recommended option. For more information about authentication, see ***Remote Authentication*** (on page 34).

- None. There is no authentication for Local Console access. This option is recommended for secure environments only.
- Select the "Ignore CC managed mode on local port" checkbox if you would like local user access to the KX II even when the device is under CC-SG management.

Note: If you initially choose not 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.



Configuring KX II Local Port Settings from the Local Console

The standard local port and the extended local port can be configured from the Remote Console on the Port Configuration page or from the Local Console on the Local Port Settings page. See ***Configuring KX II Local Port Settings*** (on page 190) for details on configuring these ports.

KX II Local Console Factory Reset

Note: This feature is available only on the KX II Local Console.

The 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, see **Audit Log**.*

To perform a factory reset:

1. Choose Maintenance > Factory Reset. The Factory Reset page opens.
2. Choose the appropriate reset option from the following options:

- Full Factory Reset - Removes the entire configuration and resets the device 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 device 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 OK button proceed. Upon completion, the KX II device is automatically restarted.

Resetting the KX II Using the Reset Button

On the back panel of the device, there is a Reset button. It is recessed to prevent accidental resets (you will need a pointed object to press this button).

The actions that are performed when the Reset button is pressed are defined in the graphical user interface. See Encryption & Share.

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, see Audit Log.

To reset the device:

1. Power off the KX II.
2. Use a pointed object to press and hold the Reset button.
3. While continuing to hold the Reset button, power the KX II device back on.
4. Continue holding the Reset button for 10 seconds. Once the device has been reset, two short beeps signal its completion.

Appendix A Specifications

In This Chapter

Physical Specifications

KX II Specifications

Part number	Line item description	UPC code	Power	Weight	Product dimensions (WxDxH)	Shipping weight	Shipping dimensions (WxDxH)
DKX2-108	8-Port KX II with 1-user network access and local port, virtual media, dual power	785813624109	Dual power 100/240 V 50/60 Hz 0.6A 25 Watts	8.58 lbs	1.75" x 17.32" x 11.4"	14.3 lbs	22" x 16.6" x 6.5"
				3.9 kg	44mm x 439mm x 290mm	6.5 kg	559mm x 422mm x 165mm
DKX2-116	16-Port KX II with 1-user network access and local port, virtual media, dual power	785813624055	Dual power 100/240 V 50/60 Hz 0.6A 25.4 Watts	8.65 lbs	1.75" x 17.3" x 11.4"	14.85 lbs	22" x 16.6" x 6.5"
				3.9 kg	44mm x 439mm x 290mm	6.7 kg	559mm x 422mm x 165mm

Part number	Line item description	UPC code	Power	Weight	Product dimensions (WxDxH)	Shipping weight	Shipping dimensions (WxDxH)
DKX2-132	32-Port KX II with 1-user network access and local port, virtual media, dual power	785813624079	Dual power 100/240 V 50/60 Hz 0.6A 26 Watts	9.0 lbs	1.75" x 17.3" x 11.4"	14.9 lbs	22" x 16.6" x 6.5"
				4.1 kg	44mm x 439mm x 290mm	6.8 kg	559mm x 422mm x 165mm
DKX2-216	16-Port KX II with 2-user network access and local port, virtual media, dual power	785813624086	Dual power 100/240 V 50/60 Hz 0.6A 26.3 Watts	8.65 lbs	1.75" x 17.3" x 11.4"	14.49 lbs	22" x 16.6" x 6.5"
				3.9 kg	44mm x 439mm x 290mm	6.6 kg	559mm x 422mm x 165mm
DKX2-232	32-Port KX II with 2-user network access and local port, virtual media, dual power	785813625021	Dual power 100/240 V 50/60 Hz (optimal 47 - 63 Hz) 0.6A 27 Watts	9.0 lbs	1.75" x 17.3" x 11.4"	14.9 lbs	22" x 16.6" x 6.5"
				4.1 kg	44mm x 439mm x 290mm	6.8 kg	559mm x 422mm x 165mm
DKX2-416	16-Port KX II with 4-user network access and local port, virtual media, dual power	785813625359	Dual power 100/240 V 50/60 Hz 1A 62 Watts	9.04 lbs	17.3” x 11.6” x 1.75”	14.94 lbs	22” x 16.5” x 6.5”
				4.1 kg	440 mm x 295 mm x 44 mm	6.8 kg	560 mm x 420 mm x 165 mm
DKX2-432	32-Port KX II with 4-user network access and local port, virtual media, dual power	785813625380	Dual power 100/240 V 50/60 Hz 1A 64 Watts	9.48 lbs	17.3” x 11.6” x 1.75”	15.38 lbs	22” x 16.5” x 6.5”
				4.3 kg	440 mm x 295 mm x 44 mm	7.0 kg	560 mm x 420 mm x 165 mm
DKX2-464	64-Port KX II with 4-user network access and local port, virtual media, dual power	785813625298	Dual power 100/240 V 50/60 Hz 1A 64 Watts	11.29 lbs	17.3” x 11.6” x 3.5”	19.8 lbs	22” x 16.5” x 6.5”
				5.12 kg	440 mm x 295 mm x 88 mm	9 kg	560 mm x 420 mm x 165 mm

KX2-8 Specifications

Part number	Line item description	UPC code	Power	Weight	Product dimensions (WxDxH)	Shipping weight	Shipping dimensions (WxDxH)
DKX2-832	32-Port KX II with 8-user network access, standard local port, extended local port, virtual media, dual power	0785813620019	Dual power 100/240 V 50/60 Hz 1A (0.5A) 64 Watts	10.57 lbs	17.3” x 14.2” x 1.73”	35.90 lbs	22” x 18.5” x 11”
				4.8 kg	440 mm x 360 mm x 44 mm	16.3 kg	560 mm x 470 mm x 280 mm
DKX2-864	64-Port KX II with 8-user network access, standard local port, extended local port, virtual media, dual power	0785813620026	Dual power 100/240 V 50/60 Hz 1.2A 64 Watts	13.22 lbs	17.3” x 14.6” x 3.5”	22.47 lbs	21.7” x 20.1” x 7.5”
				6.0 kg	440 mm x 370 mm x 88 mm	10.2 kg	550 mm x 510 mm x 190 mm

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)

Operating	
Shock	N/A

Supported Operating Systems (Clients)

The following operating systems are supported on the Virtual KVM Client and Multi-Platform Client (MPC):

Client operating system	Virtual media (VM) support on client
Windows 7®	Yes
Windows XP®	Yes
Windows 2008®	Yes
Windows Vista®	Yes
Windows 2000® SP4 Server	Yes
Windows 2003® Server	Yes
Windows 2008® Server	Yes
Red Hat® Desktop 5.0	Yes. Locally held ISO image, Remote File Server mounting directly from KX II.
Red Hat Desktop 4.0	Yes. Locally held ISO image, Remote File Server mounting directly from KX II.
Open SUSE 10, 11	Yes. Locally held ISO image, Remote File Server mounting directly from KX II.
Fedora® 8 - 11	Yes. Locally held ISO image, Remote File Server mounting directly from KX II.
Mac® OS	No
Solaris™	No

The JRE™ plug-in is available for the Windows® 32-bit and 64-bit operating systems. MPC and VKC can be launched only from a 32-bit browser, or 64-bit IE7 or IE8 browser.

Following are the Java™ 32-bit and 64-bit Windows operating system requirements.

Mode	Operating system	Browser
Windows x64 32-bit mode	Windows XP®	• Internet Explorer® 6.0 SP1+ or 7.0, IE 8 • Firefox® 1.06 - 3

Mode	Operating system	Browser
	Windows Server 2003®	• Internet Explorer 6.0 SP1++, IE 7, IE 8 • Firefox 1.06 - 3
	Windows Vista®	• Internet Explorer 7.0 or 8.0
	Windows 7®	• Internet Explorer 7.0 or 8.0 • Firefox 1.06 - 3
Windows x64 64-bit mode	Windows XP	64bit OS, 32bit browsers: • Internet Explorer 6.0 SP1+, 7.0 or 8.0 • Firefox 1.06 - 3 64bit mode, 64bit browsers: • Internet Explorer 7.0 or 8.0
	Windows XP Professional®	
	Windows XP Tablet®	
	Windows Vista	
	Windows Server 2003	
	Windows Server 2008	
	Windows 7	

Supported CIMs and Operating Systems (Target Servers)

In addition to the 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.

Supported Paragon CIMs	Operating system and serial devices (where applicable)	Virtual media	Absolute Mouse mode	Intelligent Mouse mode	Standard Mouse mode
• P2CIM-PS2	• Windows XP® • Windows 2000® • Windows 2000 Server® • Windows 2003 Server® • Windows Vista® • Windows 7® • Windows 2008® • Red Hat® Enterprise Linux® 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora® 8 - 11 • IBM® AIX™ • HP UX			✓	✓
• P2CIM-AUSB • UUSBPD	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8 - 11 • IBM AIX • HP UX • Mac® OS			✓	✓

Supported Paragon CIMs	Operating system and serial devices (where applicable)	Virtual media	Absolute Mouse mode	Intelligent Mouse mode	Standard Mouse mode
• UKVMPD (version 0C4) *Note: Version 0C5 does not work with KX II.*	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8 - 11			✓	✓
• P2CIM-SUN • P2CIM-SUSB	• All Solaris™ OSs supported in Dominion KX I				✓
• P2CIM-SER	• Serial devices				

Supported Dominion KX I DCIMs	Target server	Virtual media	Absolute Mouse mode	Intelligent Mouse mode	Standard Mouse mode
• DCIM-PS2	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora Core 3 and above • IBM AIX • HP UX			✓	✓
• DCIM-USB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8 - 11 • Mac OS • IBM AIX • HP UX			✓	✓

Supported Dominion KX I DCIMs	Target server	Virtual media	Absolute Mouse mode	Intelligent Mouse mode	Standard Mouse mode
• DCIM-USBG2	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8 - 11 • Mac OS • All Solaris OSs supported in Dominion KX I • IBM AIX • HP UX			✓	✓
Note: The DCIM-USBG2 and P2CIM-AUSB provide 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.					
• DCIM-SUN • DCIM-SUSB	• All Solaris OSs supported in Dominion KX I			✓	✓

Supported KX II D2CIMs	Target server and remote rack PDUs (where applicable)	Virtual media	Absolute Mouse mode	Intelligent Mouse mode	Standard Mouse mode
• D2CIM-VUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11 • Fedora Core 3 and above • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Mac OS	✓	✓*	✓	✓
Note: D2CIM-VUSB is not supported on Sun™ (Solaris) targets. **The Linux OS does not support Absolute Mouse mode.*					
• D2CIM-DVUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11 • Fedora 8 - 11 • Mac OS	✓	✓	✓	✓
• D2CIM-PWR	• Remote rack PDUs				

Supported Operating Systems and CIMs (KVM Target Servers)

In addition to the new D2CIMs, most Dominion 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.

Supported Dominion CIMs & D2CIMs	Operating system and serial devices (where applicable)	Virtual media	Absolute mouse mode	Intelligent mouse mode	Standard mouse mode
• DCIM-PS2 • DCIM-PS2 • DCIM-USB • DCIM-USB G2	• Windows XP® operating system • Windows 2000® operating system • Windows 2000 Server® • Windows 2003 Server® • Windows Vista® operating system			✓	✓
• D2CIM-VUSB	• Windows XP® operating system • Windows 2000® operating system • Windows 2000 Server® • Windows 2003 Server® • Windows Vista® operating system	✓		✓	✓

Target server	Supported CIMs		Mouse modes			
	Dominion DCIMs	D2CIMs	VM	AM	IM	SM
Windows XP operating system Windows 2000 operating system Windows 2000 Server®			✓	✓	✓	✓

Target server	Supported CIMs		Mouse modes			
Windows 2003 Server® Windows Vista operating system						
Red Hat® Enterprise Workstation 3.0, 4.0 and 5.0	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB (excluding Red Hat Enterprise Workstation 3.0)	✓		✓	✓
SUSE Linux Professional 9.2 and 10	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Fedora® Core 3® and above	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Mac OS	DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓		
All Solaris OSs supported in Dominion KX II	DCIM-SUN DCIM-SUSB DCIM-USB G2				✓	✓
IBM® AIX®	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
HP UX®	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
Serial Devices	Serial device support does not require a CIM				✓	

Legend:

- VM - Virtual Media (D2CIM-VUSB only)
- AM: Absolute Mouse Synchronization (D2CIM-VUSB only)
- IM: Intelligent Mouse Mode
- SM: Standard Mouse Mode
- ✓: Supported

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

Computer Interface Modules (CIMs)

Part number	Line item description	Product weight	Product dimensions (WxDxH)	Shipping weight	Shipping dimensions (WxDxH)	UPC code
D2CIM-VUSB	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
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	KX II Computer	0.2 lbs	1.3" x 3.0" x 0.6"	0.2 lbs	7.2" x 9" x	785813332011

Part number	Line item description	Product weight	Product dimensions (WxDxH)	Shipping weight	Shipping dimensions (WxDxH)	UPC code
	Interface Module for Remote Rack PDUs				0.6"	
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"x4.33"	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
D2CIM-DVUSB	Dominion KX II Computer Interface Module [Dual USB Port with Virtual Media]	0.23 lbs, 105 g	3.53”x1.68”x.76” 89.7x42.7x19.3 (mm)	.25 lbs, 112.5 g	3.9”x5.7”x 1.0” 100*145*27 (mm)	785813339508
D2CIM-DVUSB-32PAC	Bulk pack of 32 D2CIM-DVUSB	10.1 lbs, 4.6 kg	21.9”x12.2”x4.3” 555x310x110 (mm)	10.1 lbs, 4.6 kg	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

Supported Browsers

KX II supports the following browsers:

- Internet Explorer® 6, 7 and 8
- Firefox® 1.5, 2.0, and 3.0 (up to build 3.0.10)
- Safari®
- Safari® 2.0

Certified Modems

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

Devices Supported by the KX2-832 and KX2-864 Extended Local Port

The extended local port supports attachment from the following devices:

- KX2-832 and KX2-864.
- Paragon II User Station (P2-UST) connected directly to extended local port.
- Paragon II Enhanced User Station (P2-EUST) connected directly to extended local port.
- Cat5Reach URKVMG Receiver connected directly to extended local port.
- Paragon II analog KVM switch (UMT) target port connected to extended local port. Provides furthest possible access to extended local port, when used together with the Paragon II Enhanced User Station.

Target Server Connection Distance and Video Resolution

The maximum supported distance is a function of many factors including the type/quality of Cat5 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)

Note: 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.

See the ***Supported Video Resolutions*** (on page 272) for the video resolutions supported by the KX II.

KX2-832 and KX2-864 Extended Local Port Recommended Maximum Distances

Extended device	1024x768, 60 Hz	1280x1024, 60 Hz
Paragon II UMT using EUST	1000	900
Paragon EUST	500	400
URKVM	650	250
Paragon UST	500	200

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

Supported Video Resolutions

Ensure that each target server's video resolution and refresh rate are supported by the KX II and that the signal is noninterlaced.

Video resolution and cable length are important factors in the ability to obtain mouse synchronization. See ***Target Server Connection Distance and Video Resolution*** (on page 271).

The KX II supports these resolutions:

Resolutions	
640x350 @70Hz	1024x768@85

Resolutions	
640x350 @85Hz	1024x768 @75Hz
640x400 @56Hz	1024x768 @90Hz
640x400 @84Hz	1024x768 @100Hz
640x400 @85Hz	1152x864 @60Hz
640x480 @60Hz	1152x864 @70Hz
640x480 @66.6Hz	1152x864 @75Hz
640x480 @72Hz	1152x864 @85Hz
640x480 @75Hz	1152x870 @75.1Hz
640x480 @85Hz	1152x900 @66Hz
720x400 @70Hz	1152x900 @76Hz
720x400 @84Hz	1280x720@60Hz
720x400 @85Hz	1280x960 @60Hz
800x600 @56Hz	1280x960 @85Hz
800x600 @60Hz	1280x1024 @60Hz
800x600 @70Hz	1280x1024 @75Hz
800x600 @72Hz	1280x1024 @85Hz
800x600 @75Hz	1360x768@60Hz
800x600 @85Hz	1366x768@60Hz
800x600 @90Hz	1368x768@60Hz
800x600 @100Hz	1400x1050@60Hz
832x624 @75.1Hz	1440x900@60Hz
1024x768 @60Hz	1600x1200 @60Hz
1024x768@70	1680x1050@60Hz
1024x768@72	1920x1080@60Hz

Note: Composite Sync and Sync-on-Green video require an additional adapter.

Note: Some resolutions may not be available by default. If you do not see a resolution, plug in the monitor first, remove the monitor and then plug in the CIM.

Note: If the 1440x900 and 1680x1050 resolutions are not displayed but are supported by the target server's graphics adapter card, a DDC-1440 or DDC-1680 adapter may be required.

Supported Keyboard Languages

The 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 the KX II Local Console functions. For more information about non-US keyboards, see **Informational Notes** *(on page 289).*

Note: Raritan strongly recommends that you use system-config-keyboard to change languages if you are working in a Linux environment.

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
French	France	French (AZERTY) layout keyboard.
German	Germany and Austria	German keyboard (QWERTZ layout)
French	Belgium	Belgian
Norwegian	Norway	Norwegian
Danish	Denmark	Danish
Swedish	Sweden	Swedish
Hungarian	Hungary	Hungarian
Slovenian	Slovenia	Slovenian
Italian	Italy	Italian

Language	Regions	Keyboard layout
Spanish	Spain and most Spanish speaking countries	Spanish
Portuguese	Portugal	Portuguese

Smart Card Readers

Supported and Unsupported Smart Card Readers

External, USB smart card readers are supported.

Supported Smart Card Readers

Type	Vendor	Model	Verified
USB	SCM Microsystems	SCR331	Verified on local and remote
USB	ActivIdentity®	ActivIdentity USB Reader v2.0	Verified on local and remote
USB	ActivIdentity	ActivIdentity USB Reader v3.0	Verified on local and remote
USB	Gemalto®	GemPC USB-SW	Verified on local and remote
USB Keyboard/Card reader Combo	Dell®	USB Smart Card Reader Keyboard	Verified on local and remote
USB Keyboard/Card reader Combo	Cherry GmbH	G83-6744 SmartBoard	Verified on local and remote
USB reader for SIM-sized cards	Omnikey	6121	Verified on local and remote
Integrated (Dell Latitude D620)	O2Micro	OZ776	Remote only
PCMCIA	ActivIdentity	ActivIdentity PCMCIA Reader	Remote only
PCMCIA	SCM Microsystems	SCR243	Remote only

Note: SCM Microsystems SCR331 smart card readers must be using SCM Microsystems firmware v5.25.

Unsupported Smart Card Readers

This table contains a list of readers that Raritan has tested and found not to work with the Raritan device, therefore they are unsupported. If a smart card reader does not appear in the supported smart card readers table or in the unsupported smart card readers table, Raritan cannot guarantee it will function with the device.

Type	Vendor	Model	Notes
USB Keyboard/Card reader Combo	HP®	ED707A	No interrupt endpoint => not compatible with Microsoft® driver
USB Keyboard/Card reader Combo	SCM Microsystems	SCR338	Proprietary card reader implementation (not CCID-compliant)
USB Token	Aladdin®	eToken PRO™	Proprietary implementation

Minimum System Requirements

Local Port Requirements

The basic interoperability requirement for local port attachment to the KX II is:

- All devices (smart card reader or token) that are locally attached must be USB CCID-compliant.

Target Server Requirements

When using smart card readers, the basic requirements for interoperability at the target server are:

- The IFD (smart card reader) Handler must be a standard USB CCID device driver (comparable to the generic Microsoft® USB CCID driver).
- A D2CIM-DVUSB (Dual-VM CIM) is required and must be using firmware version 3A6E or later.
- Blade chassis server connections, where a CIM per blade is used, are supported.
- Blade chassis server connections, where a CIM per chassis is used, is only supported for IBM® BladeCenter® models H and E with auto-discovery enabled.

Windows XP Targets

Windows XP® operating system targets must be running Windows XP SP3 in order to use smart cards with the KX II. If you are working with .NET 3.5 in a Windows XP environment on the target server, you must be using SP1.

Linux Targets

If you are using a Linux® target, the following requirements must be met to use smart card readers with the KX II.

- CCID Requirements

  If the Raritan D2CIM-DVUSB VM/CCID is not recognized as a smart card reader by your Linux target, you may need to update the CCID driver version to 1.3.8 or above and update the driver configuration file (Info.plist).

Operating system	CCID requirements
RHEL 5	ccid-1.3.8-1.el5
SuSE 11	pcsc-ccid-1.3.8-3.12
Fedora® Core 10	ccid-1.3.8-1.fc10.i386

Remote Client Requirements

The basic requirements for interoperability at the remote client are:

- The IFD (smart card reader) Handler must be a PC/SC compliant device driver.
- The ICC (smart card) Resource Manager must be available and be PC/SC compliant.
- The JRE™ 1.6.x with smart card API must be available for use by the Raritan client application.

Linux Clients

If you are using a Linux® client, the following requirements must be met to use smart card readers with the KX II.

Note: User login to client, on smart card insertion, may take longer when 1 or more KVM sessions are actively in place to targets. As the login process to these targets is also under way.

- PC/SC Requirements

Operating system	Required PC/SC
RHEL 5	pcsc-lite-1.4.4-0.1.el5
SuSE 11	pcsc-lite-1.4.102-1.24

Fedora® Core 10	pcsc-lite-1.4.102.3.fc10.i386

- Create a Java™ Library Link

  A soft link must be created to the libpcsclite.so after upgrading RHEL 4, RHEL 5 and FC 10. For example, ln –s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so, assuming installing the package places the libraries in /usr/lib or /user/local/lib.

- PC/SC Daemon

  When the pcsc daemon (resource manager in framework) is restarted, restart the browser and MPC, too.

TCP and UDP Ports Used

Port	Description
HTTP, Port 80	This port can be configured as needed. See ***HTTP and HTTPS Port Settings*** (on page 140). By default, all requests received by the KX II via HTTP (port 80) are automatically forwarded to HTTPS for complete security. The KX II responds to Port 80 for user convenience, relieving users from having to explicitly type in the URL field to access the KX II, while still preserving complete security.
HTTPS, Port 443	This port can be configured as needed. See ***HTTP and HTTPS Port Settings*** (on page 140). By default, this port is used for multiple purposes, including the web server for the HTML client, the download of client software (MPC/VKC) onto the client's host, and the transfer of KVM and virtual media data streams to the client.
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, see Network Settings.
SNTP (Time Server) on Configurable UDP Port 123	The 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 the KX II is configured to remotely authenticate user logons 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 the KX II is configured to remotely authenticate user logons 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 the KX II is configured to remotely authenticate user logons 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 the 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).

Network Speed Settings

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	KX II: 100/Full Switch: 100/Half	100/Half	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	KX II: 100/Half Switch: 100/Full	KX II: 100/Half Switch: 100/Full	100/Full	KX II: 100/Half Switch: 100/Full	No Communication	No Communication
	100/Half	100/Half	100/Half	KX II: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
	10/Full	KX II: 10/Half Switch: 10/Full	No Communication	No Communication	No Communication	10/Full	KX II: 10/Half Switch: 10/Full
	10/Half	10/Half	No Communication	No Communication	No Communication	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 KX II behavior deviates from expected behavior

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

When an LDAP/LDAPS authentication is successful, the 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.

In addition, for Microsoft® Active Directory®, the standard LDAP memberOf is used.

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® operating system server requires updating the LDAP/LDAPS schema. See your Microsoft documentation for details.

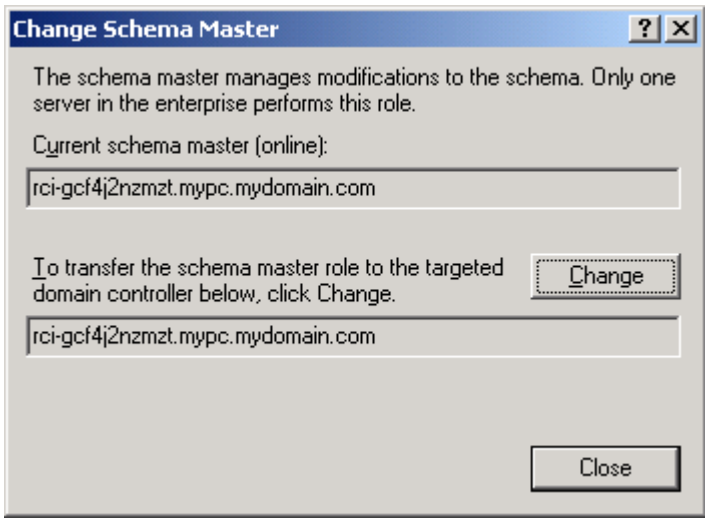
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

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.



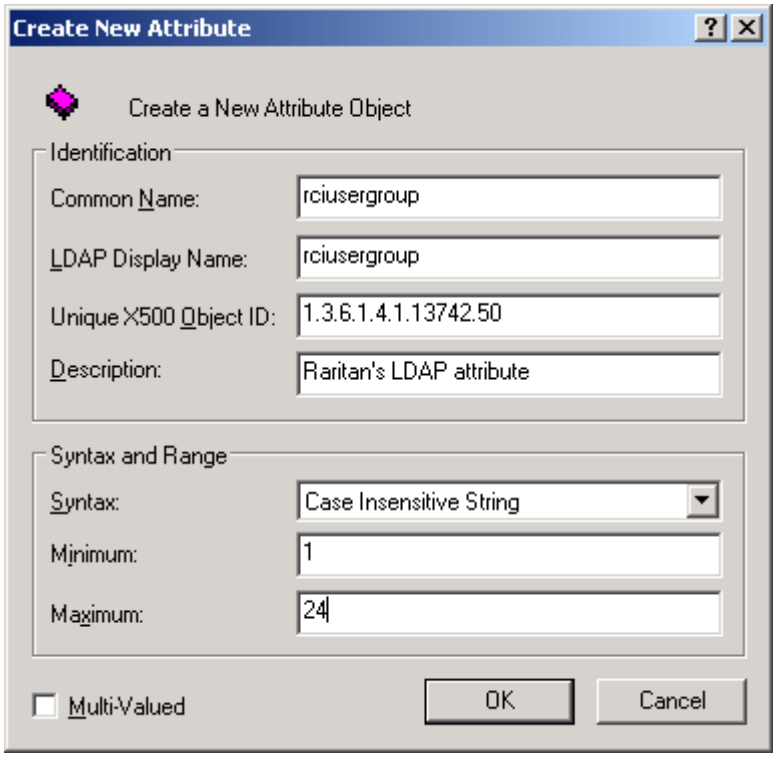
2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**
3. Click OK.

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.



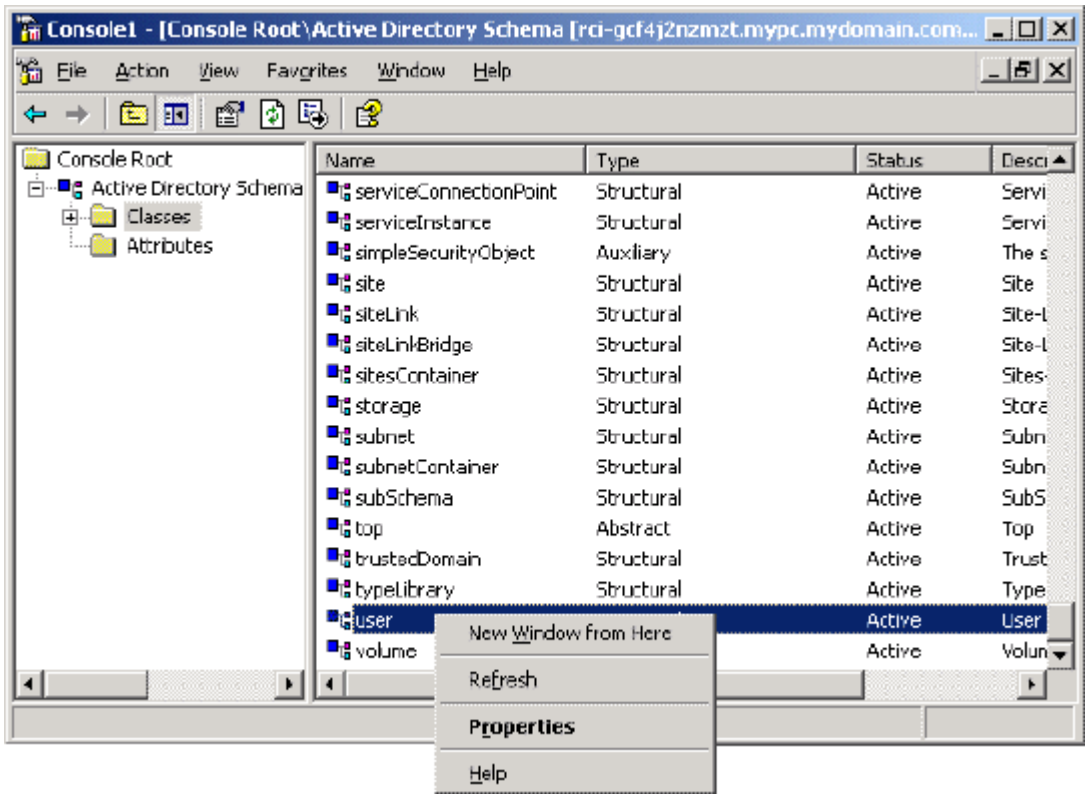
4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String 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.



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.
2. Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

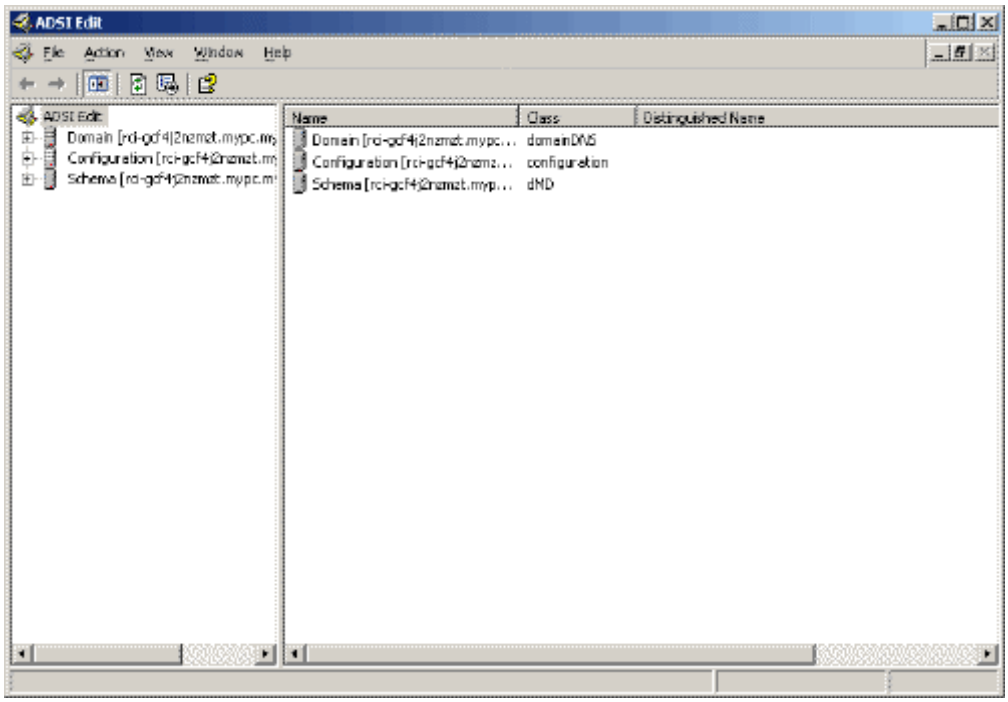
Editing rciusergroup Attributes for User Members

To run the Active Directory® script on a 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:

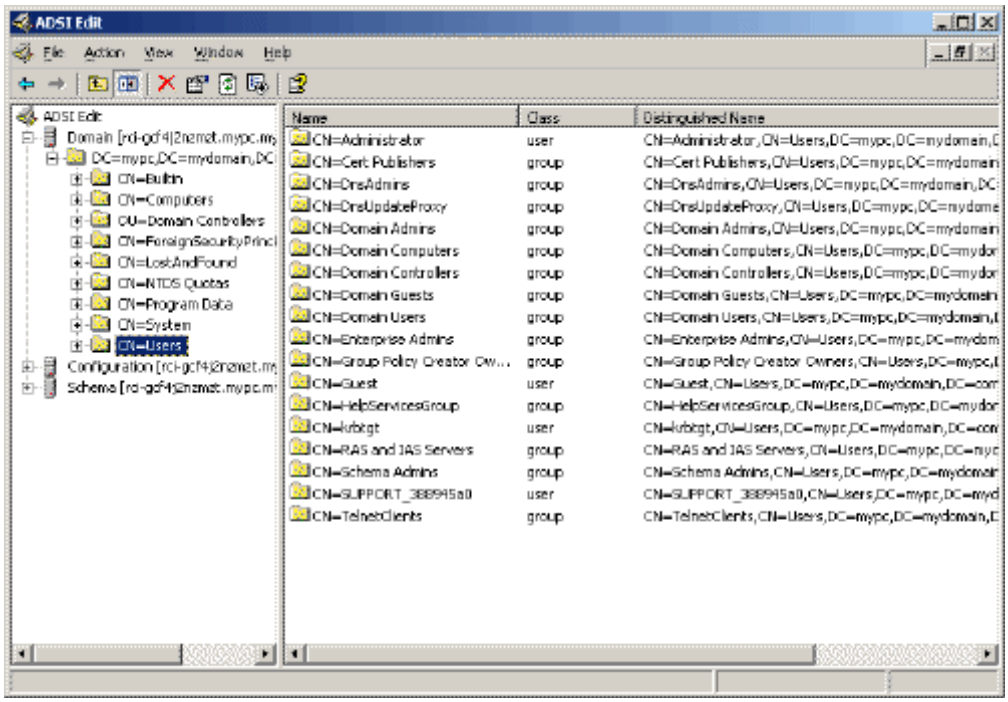
1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.

3. Go to the directory where the support tools were installed. Run adsiedit.msc. The ADSI Edit window opens.

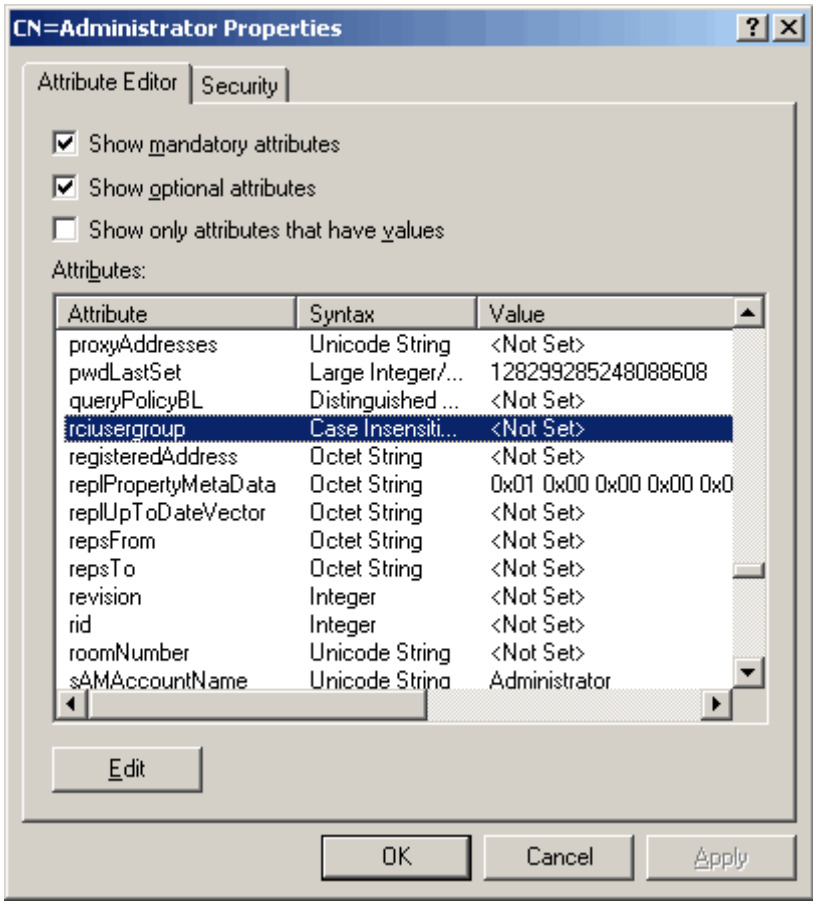


4. Open the Domain.

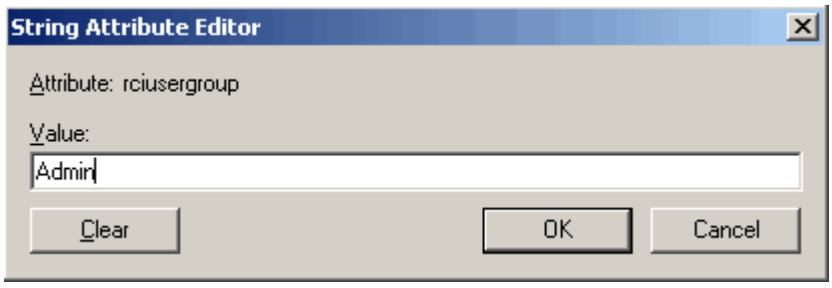
5. In the left pane of the window, select the CN=Users folder.



6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.
7. Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.



8. Click Edit. The String Attribute Editor dialog appears.
9. Type the user group (created in the KX II) in the Edit Attribute field. Click OK.



Appendix C Informational Notes

In This Chapter

Overview

This section includes important notes on KX II usage. Future updates will be documented and available online through the Help link in the KX II Remote Console interface.

Java Runtime Environment (JRE)

Important: It is recommended that you disable Java™ caching and clear the Java cache. Please refer to your Java documentation or the KVM and Serial Access Clients Guide for more information.

The KX II Remote Console and MPC require the Java Runtime Environment™ (JRE™) to function. The 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 JRE version 1.6 for optimum performance, but the KX II Remote Console and MPC will function with JRE version 1.6.x and higher with the exception of 1.6.2.

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

IPv6 Support Notes

Java

Java™ 1.6 supports IPv6 for the following:

- Solaris™ 8 and higher
- Linux® kernel 2.1.2 and higher (RedHat 6.1 and higher)

Java 5.0 and above supports the IPv6 for the following:

- Solaris 8 and higher
- Linux kernel 2.1.2 and higher (kernel 2.4.0 and higher recommended for better IPv6 support)
- Windows XP® SP1 and Windows 2003®, Windows Vista® operating systems

The following IPv6 configurations *are not* supported by Java:

- J2SE 1.4 does not support IPv6 on Microsoft® Windows®.

Linux

- It is recommended that Linux kernel 2.4.0 or higher is used when using IPv6.
- An IPv6-enabled kernel will need to be installed or the kernel will need to be rebuilt with IPv6 options enabled.
- Several network utilities will also need to be installed for Linux when using IPv6. For detailed information, refer to http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html

Windows

- Windows XP and Windows 2003 users will need to install the Microsoft IPV6 service pack to enable IPV6.

Mac Leopard

- IPv6 is not supported in KX II version 2.0.20 for Mac® Leopard®.

Samba

- IPv6 is not supported for use with virtual media when using Samba.

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® Operating System 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.

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)
Slovenian	System Settings (Control Center)
Italian	System Settings (Control Center)
Portuguese	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.

Dell Chassis Cable Lengths and Video Resolutions

In order to maintain video quality, Raritan recommends using the following cable lengths and video resolutions when you are connecting to Dell® blade chassis from the KX II:

Cable length	Video resolution
50 ft.	1024x768x60
50 ft.	1280x1024x60
30 ft.	1600x1200x60

Fedora

Resolving Fedora Core Focus

Using the Multi-Platform Client (MPC), occasionally there is an inability to log in to a 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.

Mouse Pointer Synchronization (Fedora)

When connected in dual mouse mode to a target server running Fedora® 7, If the target and local mouse pointers lose synchronization, changing the mouse mode from or to Intelligent or Standard may improve synchronization. Single mouse mode may also provide for better control.

To resynchronize the mouse cursors:

- Use the Synchronize Mouse option from the Virtual KVM Client.

VKC and MPC Smart Card Connections to Fedora Servers

If you are using a smart card to connect to a Fedora® server via MPC or VKC upgrade the pcsc-lite library to 1.4.102-3 or above.

Resolving Issues with Firefox Freezing when Using Fedora

If you are accessing Firefox® and are using a Fedora® server, Firefox may freeze when it is opening. To resolve this issue, install the libnpjp2.so Java™ plug-in on the server.

Video Modes and Resolutions

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). The 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 KX II.

Supported Video Resolutions Not Displaying

When using a CIM, there are some video resolutions, as listed in ***Supported Video Resolutions*** (on page 272), that may not be available to you for selection by default.

To view all available video resolutions if they do not appear:

1. Plug the monitor in.
2. Next, unplug the monitor and plug in the CIM. All video resolutions will not be available and can be used.

USB Ports and Profiles

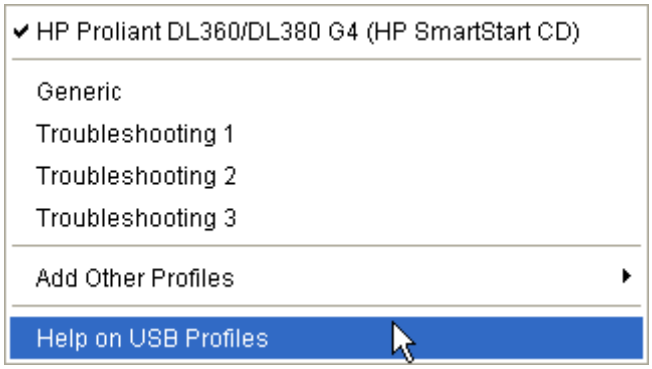
VM-CIMs and DL360 USB Ports

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 102).

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 (for example, Linux®, MAC OS-X®).

There are also a number of profiles (designated by platform name and BIOS revision) that have been tailored to enhance the 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, manufacturer, and version.
    b. The intended use (e.g. redirecting an image to reload a server's operating system from CD).

Changing a USB Profile when Using a Smart Card Reader

There may be certain circumstances under which you will need to change the USB profile for a target server. For example, you may need to change the connection speed to "Use Full Speed for Virtual Media CIM" when the target has problems with the "High Speed USB" connection speed.

When a profile is changed, you may receive a New Hardware Detected message and be required to log in to the target with administrative privileges to reinstall the USB driver. This is only likely to occur the first few times the target sees the new settings for the USB device. Afterward, the target will select the driver correctly.

CIMs

Windows 3-Button Mouse on Linux Targets

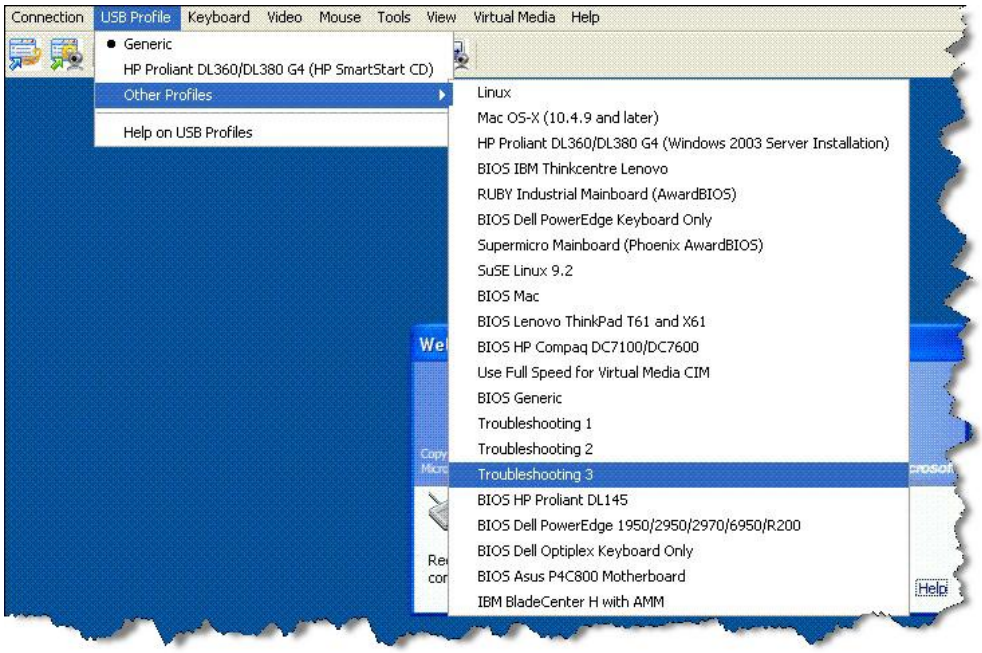
When using a 3-button mouse on a Windows® client connecting to a Linux® target, the left mouse button may get mapped to the center button of the Windows client 3-button mouse.

Windows 2000 Composite USB Device Behavior for Virtual Media

The Windows 2000® operating system does not support USB composite devices, like Raritan's D2CIM-VUSB, in the same manner as non-composite USB devices.

As a result, the "Safely Remove Hardware" system tray icon does not appear for drives mapped by the D2CIM-VUSB and a warning message may appear when disconnecting the device. Raritan has not observed any problems or issues from this message, however.

Raritan's US engineering department has developed a configuration which supports the "Safely Remove Hardware" icon and avoids this Windows message. This configuration requires the use of the D2CIM-DVUSB virtual media adapter and the Troubleshooting 3 USB Profile, which configures the D2CIM-DVUSB as a non-composite USB device supporting a single virtual media connection. Raritan has successfully tested this configuration in the US and Japan.



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.

Accessing Virtual Media on a Windows 2000 Server Using a D2CIM-VUSB

A virtual media local drive cannot be accessed on a Windows 2000® server using a D2CIM-VUSB.

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.

Virtual Media Connection Failures Using High Speed for Virtual Media Connections

Under certain circumstances it may be necessary to select the "Use Full Speed for Virtual Media CIM" when a target has problems with "High Speed USB" connections or when the target is experiencing USB protocol errors caused by signal degradation due to additional connectors and cables (for example, a connection to a blade server via a dongle).

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”.

Single Mouse Mode - Connecting to a KX II Target Under CC-SG Control Via VKC Using Firefox

When using Firefox® to connect to a KX II target under CC-SG control using DCIM-PS2 or DCIM-USBG2, if you change to Single Mouse Mode in the Virtual KVM Client, the VKC window will no longer be the focus window and the mouse will not respond. If this occurs, left click on the mouse or press Alt+Tab to return the focus to the VKC window.

Proxy Mode and MPC

If you are using 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).

Moving Between Ports of the KX II

If you move a between ports of the same KX II and resume management within one minute, CC-SG may display an error message. If you resume management, the display will be updated.

Appendix D FAQs

In This Chapter

General Questions

What is the KX II?

The KX II is a second generation digital KVM (keyboard/video/ mouse) switch that enables one, two, four or eight IT administrators to access and control 8, 16, 32 or 64 servers over the network with BIOS-level functionality. The KX II is completely hardware and operating system independent. Users can troubleshoot and reconfigure servers even when servers are down.

At the rack, the KX II provides the same functionality, convenience, space savings, and cost savings as traditional KVM switches. However, the 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 the KX II differ from remote control software?

When using the KX II remotely, the interface, at first glance, may seem similar to remote control software such as pcAnywhere™, Windows Terminal Services/Remote Desktop®, VNC, and so forth. However, because the KX II is not a software but a hardware solution, it's much more powerful. Specifically:

- OS- and hardware-independent - The KX II can be used to manage servers running many popular operating systems, including Intel®, Sun™, PowerPC running Windows®, Linux®, Solaris™, etc.
- State-Independent/Agentless - The KX II does not require the managed server's operating system 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 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 KX II still works flawlessly to enable these configurations to be made.

How do the new features of the KX II compare to the KX I?

The 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 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 KX II models. Raritan's centralized management unit, CommandCenter Secure Gateway, and the Multi-Platform Client (MPC) both support KX I and KX II switches seamlessly.

Will my existing KX I CIMs work with the KX II switches?

Yes, existing KX I CIMs will work with the KX II switch. In addition, select Paragon CIMs will work with the KX II. This provides an easy migration to the KX II from Paragon I customers who wish to switch to KVM-over-IP. However, you may want to consider the D2CIM-VUSB and D2CIM-DVUSB CIMs which support Virtual Media and Absolute Mouse Synchronization.

Can the KX II be rack mounted?

Yes. The 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 KX II?

The KX II is only 1U high (except KX2-864 and KX2-464, which are 2U), fits in a standard 19" rack mount, and is only 11.4" (29 cm) deep. The Dominion KX2-832 and KX2-864 are 13.8"" (44 cm) deep.

Remote Access

How many users can remotely access servers on each KX II?

The KX II models offer remote connections for up to eight users per user channel to simultaneously access and control 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. Likewise, for the eight channel devices, up to eight users can access a single server, up to an overall maximum of 32 users across the 8 channels.

Can two people look at the same server at the same time?

Yes, 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 the KX II from a client, what hardware, software or network configuration is required?

Because the KX II is completely web-accessible, it doesn't require installation of proprietary software on clients used for access. An optional installed client is available on Raritan.com and is required for access by external modem.

The KX II can be accessed through major Web browsers, including: Internet Explorer, Mozilla and Firefox. Dominion KX II can now be accessed on Windows, Linux and Macintosh desktops, via Raritan's new Windows Client, and the Java-based Multiplatform and Virtual KVM Clients.

KX II administrators can perform remote management functions, such as set passwords and security, rename servers, change IP address and so on, using a convenient browser-based interface.

What is the file size of the Virtual KVM Client applet that is used to access the KX II? How long does it take to retrieve?

The Virtual KVM Client applet used to access the KX II is approximately 500KB in size. The following chart describes the approximate time required to retrieve the 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 the KX II if the network ever becomes unavailable?

You can access servers at-the-rack or via modem. The KX II offers a dedicated modem port for attaching an external modem.

Do you have a Windows® client?

Yes, in Release 2.2, we have a native .NET Windows Client, which is called the Raritan Active KVM Client.

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 KX II switches. MPC can be run via web browser and standalone. Refer to Virtual KVM Client and Raritan Multi-Platform Client (MPC) Supported Operating Systems in the KVM and Serial Client Guide for more information.

Do your KVM clients support LCD monitors?

Yes. For customers wishing to enhance their productivity by using multiple LCD monitors on their desktops, the KX II can launch KVM sessions to multiple monitors, either in full screen or standard modes.

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 KX II models support virtual media?

All of the KX II models support virtual media. It is available standalone and through Raritan's CommandCenter Secure Gateway, Raritan's centralized management unit.

What types of virtual media does the KX II support?

The 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.

What is required for virtual media?

A 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 should be purchased by customers who wish to utilize virtual media at the BIOS level. The D2CIM-DVUSB is also required for smart card authentication.

The D2CIM-VUSB has a single USB connector and is for customers who will use virtual media at the OS level.

Both support virtual media sessions to target servers supporting the USB 2.0 interface.

Available in economical 32 and 64 quantity CIM packages, these CIMs support Absolute Mouse Synchronization as well as remote firmware update.

Is virtual media secure?

Yes. Virtual media sessions are secured using AES or RC4 encryption.

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 KX II's USB interface to the server to accommodate these server specific characteristics.

Why would I use a USB profile?

USB Profiles are most often required at the BIOS level where there may not be full support for the USB specification when accessing virtual media drives.

However, profiles are sometimes used at the operating system level, for example, for mouse synchronization for Mac® and Linux® servers.

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 KX II's Port Configuration pages.

A USB profile can also be selected in the 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 102).

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 102). 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.

Bandwidth and KVM-over-IP Performance

How is bandwidth used in KVM-over-IP systems?

The 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 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 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 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 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 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 KX II's default bandwidth settings and with two reduced bandwidth settings (Connection Speed setting of 1Mbit with 15 and 8 bit color) on a Windows XP target server (1024x768 resolution) over a 100 Mbit/s LAN:

User task	Default	1Mbit speed & 15 bit color	1Mbit 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
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 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 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 maximum remote (over IP) video resolution supported?

The KX II is the first and only KVM-over-IP switch to support full High Definition (HD) remote video resolution – 1920x1080.

In addition, popular widescreen formats are supported, including 1600x1200, 1680x1050 and 1440x900, so remote users can work with today's higher resolution monitors.

What about servers with DVI ports?

Servers with DVI ports that support DVI-A (analog) and DVI-I (integrated analog and digital) can use a simple, passive adapter such as the ADVI-VGA to convert the DVI port to a VGA plug that can be connected to a KX II CIM's VGA plug.

Servers with DVI ports that only support DVI-D (digital) would need a more expensive adapter, but customers should check to see if the server's video card can be configured to support DVI-I or DVI-A.

Ethernet and IP Networking

Does the KX II offer dual gigabit Ethernet ports to provide redundant fail-over?

Yes. The 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 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.

What is the speed of the KX II's Ethernet interfaces?

The KX II supports gigabit as well as 10/100 Ethernet. The KX II supports two 10/100/1000 speed Ethernet interfaces, with configurable speed and duplex settings (either autodetected or manually set).

Does the KX II offer dual gigabit Ethernet ports to provide redundant failover or load balancing?

Yes. 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, 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.

Can I access the KX II over a wireless connection?

Yes. The 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 KX II, servers can be configured and managed at BIOS-level wirelessly.

Can the 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 KX II's KVM-over-IP technology can accommodate the connection.

Can I use the KX II with a VPN?

Yes, the KX II uses standard Internet Protocol (IP) technologies from Layer 1 through Layer 4. Traffic can be easily tunneled through standard VPNs.

Can I use KX II with a proxy server?

Yes. The KX II can be used with a SOCKS proxy server, assuming the remote client PC is configured appropriately. Contact the user documentation or online help for more information.

How many TCP ports must be open on my firewall in order to enable network access to the KX II? Are these ports configurable?

Only one. The 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 KX II's optional web browser capability, the standard HTTPS port 443 must also be open.

Does the KX II require an external authentication server to operate?

No. The KX II is a completely self-sufficient. After assigning an IP address to the KX II, it is ready to use. Its web browser and authentication capabilities are completely built-in.

If an external authentication server (such as LDAP, Active Directory, RADIUS, etc.) is used, the 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 KX II's design philosophy is optimized to provide ease of installation, complete independence from any external server, and maximum flexibility.

Can the KX II be used with CITRIX?

The 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 KX II use DHCP?

DHCP addressing can be used, however, Raritan recommends fixed addressing since the 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 KX II over my IP network. What could be the problem?

The 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 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 KX II is the same as another device, network connectivity may be inconsistent.
- Port 5000 conflicts - If another device is using port 5000, the KX II default port must be changed (or the other device must be changed).

When changing the IP address of the KX II or swapping in a new KX II, sufficient time must be allowed for its IP and MAC addresses to be known throughout the Layer 2 and Layer 3 networks.

IPv6 Networking

What is IPv6?

IPv6 is the acronym for “Internet Protocol Version 6”. IPv6 is the “next generation” IP protocol which will replace the current IP Version 4 (IPv4) protocol.

IPv6 addresses a number of problems in IPv4, such as the limited number of IPv4 addresses. It also improves IPv4 in areas such as routing and network auto-configuration. IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years.

IPv6 helps one of the largest headaches of an IP network from the administrator’s point of view; configuring and maintaining an IP network.

Why does the KX II support IPv6 networking?

US government agencies and the Department of Defense are now mandated to purchase IPv6 compatible products. In addition, many enterprises and foreign countries such as China will be transitioning to IPv6 over the next several years.

What is "dual stack" and why is it required?

Dual stack is the ability to simultaneously support both IPv4 and IPv6 protocols. Given the gradual transition from IPv4 to IPv6, dual stack is a fundamental requirement for IPv6 support.

How do I enable IPv6 on the KX II?

Use the Network Settings page, available from the Device Settings menu in KX II. Enable IPv6 addressing and choose manual or auto-configuration. You must also enable it in MPC.

What if I have an external server with an IPv6 address that I want to use with my KX II?

The KX II can access external servers via their IPv6 addresses, for example, an SNMP Manager, Syslog server, or LDAP server.

Using the KX II’s dual-stack architecture, these external servers can be accessed via (1) an IPv4 address, (2) IPv6 address or (3) hostname. So the KX II supports the mixed IPv4/IPv6 environment many customers will have.

Does the Dominion KX I support IPv6?

No, the Dominion KX I does not support IPv6 addresses.

What if my network doesn't support IPv6?

The KX II’s default networking is set at the factory for IPv4 only. When you are ready to use IPv6, then follow the above instructions to enable IPv6/IPv4 dual stack operation.

Where can I get more information on IPv6?

See www.ipv6.org for general information on IPv6. The KX II User Guide describes the KX II's support for IPv6.

Servers

Does the 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 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 KX II is completely independent. Even if a user chooses to configure the KX II to authenticate against an Active Directory server - if that Active Directory server becomes unavailable, the 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 KX II's web browser capability?

No. The KX II is a completely self-sufficient device. After assigning an IP address to the 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 KX II from a particular workstation?

None. The KX II can be accessed completely via a web browser. However, there is an optional installed client provided on Raritan's website (www.raritan.com), which is required for modem connections. A Java-based client is now available for non-Windows users.

What should I do to prepare a server for connection to the 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.

What about mouse synchronization?

For many KVM-over-IP users, mouse synchronization is a frustrating experience. The KX II's Absolute Mouse Synchronization provides for a tightly synchronized mouse without requiring server mouse setting changes on Windows and Apple® Mac® servers. For other servers, the Intelligent Mouse mode or the speedy, single mouse mode can be used to avoid changing the server mouse settings.

Blade Servers

Can I connect blade servers to the KX II?

Yes. The KX II supports popular blade server models from the leading blade server manufacturers: HP®, IBM® and Dell®.

Which blade servers are supported?

The following models are supported:

- Dell® PowerEdge® 1855, 1955 and M1000e
- HP BladeSystem c3000 and c7000
- IBM® BladeCenter® H and E

Note: IBM BladeCenter Model S, T, and HT are handled using the IBM (Other) selection.

Are the Paragon Blade CIMs used?

No, the Paragon II Blade CIM will not work with the KX II.

Which CIM should I use?

It depends on the type of KVM ports on the specific make and model of the blade server you are using. The following CIMs are supported: DCIM-PS2, DCIM-USBG2, D2CIM-VUSB and D2CIM-DVUSB.

What types of access and control are available?

The KX II provides automated & secure KVM access: (1) at-the-rack, (2) remotely over IP, (3) via CommandCenter and (4) by modem.

Do I have to use hotkeys to switch between blades?

Some blade servers require you to use hotkeys to switch between blades. With the KX II, you don't have to use these hotkeys. Just click on the name of the blade server and the KX II will automatically switch to that blade without the explicit use of the hotkey.

Can I access the blade server's management module?

Yes, you can define the URL of the management module and access it from the KX II or from CC-SG. If configured, one-click access is available.

How many blade servers can I connect to a KX II?

For performance and reliability reasons, you can connect up to 8 blade chassis to a KX II (regardless of model) or up to 4 for a KSX II.

For KX II's, Raritan recommends connecting up to two times the number of remote connections supported by the device. For example, with a KX2-216 with two remote channels, we recommend connecting up to 4 blade server chassis. You can of course connect individual servers to the remaining server ports.

I'm an SMB customer with a few KX II's. Must I use your CC-SG management station?

No, you don't have to. SMB customers are not required to use CC-SG to use the new blade features.

I'm an enterprise customer using CC-SG. Can I access blade servers via CC-SG?

Yes. Once blade servers are configured on the KX II, the CC-SG user can access them via KVM connections. In addition the blade servers are organized by chassis as well as CC-SG custom views.

What if I want in-band or embedded KVM access?

Yes, in-band and embedded access to blade servers can be configured within CC-SG.

I'm running VMware on some of my blade servers. Is this supported?

Yes, with CC-SG you can display and access virtual machines running on blade servers.

Is virtual media supported?

We support VM on IBM BladeCenter® Model H and E with the D2CIM - DVUSB.

Is Absolute Mouse Synchronization supported?

Servers with internal KVM switches inside the blade chassis typically do not support absolute mouse technology. For HP Blade and some Dell blade servers, the CIM is connected to each blade, so absolute mouse is supported if the underlying OS running on the blade does.

Is blade access secure?

Yes, blade access uses all of the standard KX II security features such as 128 bit or 256 bit encryption. In addition, there are blade-specific security features such as per blade access permissions and hot key-blocking that eliminates un-authorized access.

Installation

Besides the device itself, what do I need to order from Raritan to install the KX II?

Each server that connects to the 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 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 KX II.

What types of servers can be connected to the KX II?

The 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 KX II?

Servers that connect to the 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 the KX II using standard UTP (twisted pair) cable such as Cat5, Cat5e, or Cat6.

How far can my servers be from the KX II?

In general servers can be up to 150 feet (45 m) away from the KX II depending on the type of server. Refer to the Raritan website (www.raritan.com) or Target Server Connection Distance and Video Resolution for more information. For the new D2CIM-VUSB and D2CIM-DVUSB CIMs that support 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 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 KX II?

Servers connected to the KX II do not require any software agents to be installed, because the KX II connects directly via hardware to servers' keyboard, video, and mouse ports.

How many servers can be connected to each the KX II device?

The 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 the KX II and reconnect it to another KX II device, or connect it to a different port on the same KX II device?

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 the 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 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 KX II functions just like a traditional KVM switch, allowing control of up to 64 servers using a single keyboard, monitor, and mouse.

Can I consolidate the local ports of multiple KX II's?

Yes. You can connect the local ports of multiple KX II switches to another KX II using the "tiering" feature of the KX II. You can then access the servers connected to your KX II devices from a single point in the data center via a consolidated port list.

When I am using the local port, do I prevent other users from accessing servers remotely?

No. The 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 KX II has USB keyboard and mouse ports on the local port. Note that as of April 2011, the Dominion KX II switches will no longer have PS/2 local ports. Customers with PS/2 keyboard and mice should utilize a PS/2 to USB adapter.

Is there an onscreen display for local, at-the-rack access?

Yes, but the KX II's at-the-rack access goes way beyond conventional GUIs. Featuring the industry's first browser-based interface for at-the-rack access, the 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 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 KX II fails-over to its own internal authentication database.

The 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 KX II onscreen display is changed, this updates all remote clients and external management servers in real-time.

If I use the KX II's remote administration tools to change the name of a connected server, does that change propagate to the local port GUI 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 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.

Extended Local Port (Dominion KX2-832 and KX2-864 Models Only)

What is the extended local port?

The Dominion KX2-832 and KX2-864 feature an extended local port. The KX II eight user models have a standard local port, plus a new extended local port that extends the local port, via Cat5 cable, beyond the rack to a control room, another point in the data center or to a Paragon II switch.

Can I connect the extended local port to another KX II?

Yes, you can connect the extended local port to a server port of another KX II using the "tiering" feature of the KX II.

Is a user station required for the extended local port?

Yes, the following devices can function as the "user station" for the extended local port: Paragon II EUST, Paragon II UST, and the Cat5 Reach URKVMG device. In addition, the extended local port can be connected via Cat5 cable to a server port on a Paragon II switch. This configuration can be used to consolidate the local ports of many KX2-8xxx devices to a single switch.

How far can the user station be from the KX II?

The distance is 200' to 1000', but varies according to the type of user station, the video resolution, cable type and quality.

Is a CIM required?

No CIM is required. Just connect a Cat5 cable.

Must I use the extended local port?

No, the extended local port is an optional feature and is disabled by default. Use the Local Port Settings page to enable it. You can also disable the standard local port if you are not going to use it for added security.

Power Control

Does the KX II have a dual power option?

All of the 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 KX II will automatically switch to the other.

Does the power supply used by the KX II automatically detect voltage settings?

Yes. The 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 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 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 KX II offer?

Raritan's Remote Power Control power strips can be connected to the 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.

How many PDUs can be connected to a KX II?

Up to eight PDUs can be connected to a KX II device.

How do I connect the PDU to the KX II?

The D2CIM-PWR is used to connect the power strip to the KX II. The D2CIM-PWR must be purchased separately; it does not come with the PDU.

Does the KX II support servers with multiple power supplies? What if each power supply is connected to a different rack PDU (power strip)?

Yes. The 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 KX II device. Four power supplies can be connected per target server to multiple power strips.

Does the KX II display statistics and measurements from the PDU?

Yes. PDU-level power statistics, including power, current and voltage, are retrieved from the PDU and displayed to the user.

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. For these servers, see the server's documentation to change this setting.

What happens when I recycle power to a server?

This is the physical equivalent of unplugging the server from the AC power line, and reinserting the plug.

Can I power on/off other equipment (non-servers) connected to a PDU?

Yes. You can power on/off other equipment attached to the PDU by outlet from the Dominion KX II's browser-based interface.

What type of rack PDUs does the KX II support?

To take advantage of the 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 KX II.

Scalability

How do I physically connect multiple KX II devices together into one solution?

To physically connect multiple KX II devices together for consolidated local access, you can connect the local ports of multiple "tiered" (or "cascaded") KX II switches to a "base" KX II using the "tiering" feature of the KX II. You can then access the servers connected to your KX II devices from a single point in the data center via a consolidated port list.

The D2CIM-DVUSB CIM must be used to connect the "tiered" KX II switch to the "base" switch. Or for the KX2-832 and KX2-864, the extended local port can be connected via CAT5/6 cable (no CIM required) to the base KX II switch.

Access via the consolidated port list is available in the data center or even from a remote PC. All servers connected to the tiered KX II's can be accessed via a hierarchical port list or via search (with wildcards).

Two levels of tiering are supported; up to 1024 devices can be accessed in a tiered configuration. Remote power control is also supported.

Virtual media, smart card and blade server access via tiered access will be supported in a future release. Of course these features are available when accessed via a standard remote connection.

While remote IP server access via the consolidated port list is available as a convenience, accessing the tiered server from CommandCenter or directly via the KX II the server is connected to is recommended for optimal performance.

Do I have to physically connect KX II devices together?

Multiple KX II units do not need to be physically connected together. Instead, each KX II unit connects to the network, and they automatically work together as a single solution if deployed with Raritan's CommandCenter Secure Gateway (CC-SG) management appliance.

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.

Customers using CC-SG for centralized remote access can make good use of the KX II's tiering (cascading) feature to consolidate the local ports of multiple KX II switches and locally access up to 1024 servers from a single console when in the data center.

Is CC-SG required?

For customers wanting stand-alone usage (without a central management system), multiple KX II units still interoperate and scale together via the IP network. Multiple KX II switches can be accessed from the KX II web-based user interface and from the Multiplatform Client (MPC).

Can I connect an existing analog KVM switch to the KX II?

Yes. Analog KVM switches can be connected to one of the KX II's server ports. Simply use a D2CIM-DVUSB or D2CIM-VUSB 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 KX II?

Yes. Certain Paragon computer interface modules (CIMs) may work with the KX II (check the Raritan KX II release notes on the website for the latest list of certified CIMs).

However, because Paragon CIMs cost more than 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 KX II. Also note that when connected to the KX II, Paragon CIMs transmit video at a distance of up to 150 feet, the same as the KX II CIMs; not at 1000 feet [300 meters], as they do when connected to Paragon.

Can I use the KX II Computer Interface Modules (CIMs) with Raritan's analog matrix KVM switch, Paragon?

No. The 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.

Does the KX II support Paragon Dual CIMs?

Yes. The KX II now supports Paragon II Dual CIMs (P2CIM-APS2DUAL and P2CIM-AUSBDUAL), which can connect servers in the data center to two different KX II switches.

If one KX II switch is not available, the server can be accessed through the second KX II switch, providing redundant access and doubling the level of remote KVM access.

Please note these are Paragon CIMs, so they do not support the KX II advanced features such as virtual media, absolute mouse, and so on.

Security

Is the Dominion KX II FIPS 140-2 Certified?

The KX II 2.2.0 and later, and the KSX II 2.3.0 and later, provides users with the option to use an embedded FIPS 140-2-validated cryptographic module running on a Linux platform per FIPS 140-2 implementation guidelines. This cryptographic module is used for encryption of KVM session traffic consisting of video, keyboard, mouse, virtual media and smart card data.

What kind of encryption does the KX II use?

The KX II uses industry-standard (and extremely secure) 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 KX II that is not completely secured by encryption.

Does the KX II support AES encryption as recommended by the US Government's NIST and FIPS 140-2 standards?

The 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 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 KX II does not compromise security; it allows encryption of keyboard, mouse and video data.

How does the KX II integrate with external authentication servers such as Active Directory®, RADIUS, or LDAP?

Through a very simple configuration, the 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 KX II receives the user group to which that user belongs from the authentication server. The 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 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 KX II support strong password?

Yes, the 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 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.

Can I upload my own digital certificate to the KX II?

Yes. Customers can upload self-signed or certificate authority-provided digital certificates to the KX II for enhanced authentication and secure communication.

Does the KX II support a configurable security banner?

Yes. For government, military and other security conscious customers requiring a security message before user login, the KX II can display a user-configurable banner message and optionally require acceptance.

My security policy does not allow the use of standard TCP port numbers. Can I change them?

Yes. For customers wishing to avoid the standard TCP/IP port numbers to increase security, the KX II allows the administrator to configure alternate port numbers.

Smart Cards and CAC Authentication

Does the KX II support smart card and CAC authentication?

Yes, smart cards and DoD Common Access Card (CAC) authentication to target servers is supported in release KX II 2.1.10 and later, and KSX II 2.3.0 and later.

What KX II models support smart cards/CAC?

All KX II models are supported. The Dominion KX II-101 does not currently support smart cards and CAC.

Do enterprise and SMB customers use smart cards, too?

Yes. However, the most aggressive deployment of smart cards is in the U.S. federal government.

What CIMs support smart cards/CAC?

The D2CIM-DVUSB is required. This CIM must be upgraded with the release 2.1.10 and later of the firmware, and KSX II 2.3.0 and later.

What firmware version is required?

The KX II release 2.1.10 and later or and KSX II 2.3.0 and later are required.

What smart card readers are supported?

The required reader standards are USB CCID and PC/SC. See ***Supported and Unsupported Smart Card Readers*** (on page 275).

Can smart card/CAC authentication work on the local port and via Command Center?

Yes. For the local port, connect a compatible smart card reader to the USB port of the KX II.

Are the Paragon smart card enabled UST and CIM used?

No, the P2-EUST/C and P2CIM-AUSB-C are not part of the KX II solution.

Manageability

Can the KX II be remotely managed and configured via web browser?

Yes, the 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 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 KX II's default IP address, you can even configure the initial settings via web browser.)

Can I backup and restore the KX II's configuration?

Yes, the KX II's device and user configurations can be completely backed up for later restoration in the event of a catastrophe.

The KX II's backup and restore functionality can be used remotely over the network or via the Remote Console.

What auditing or logging does the KX II offer?

For complete accountability, the 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 KX II integrate with Syslog?

Yes. In addition to the KX II's own internal logging capabilities, the KX II can send all logged events to a centralized Syslog server.

Can the KX II integrate with SNMP?

Yes. In addition to the KX II's own internal logging capabilities, the KX II can send SNMP traps to SNMP management systems like HP OpenView and Raritan's CC-NOC.

Can the KX II's internal clock be synchronized with a timeserver?

Yes, the 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 KX II's default IP address?

192.168.0.192

What is the KX II's default user name and password?

The 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 KX II forces the administrator to change the KX II default administrative user name and password when the unit is first booted up.

I changed and subsequently forgot the KX II's administrative password; can you retrieve it for me?

The 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 KX II using Firefox®, and I opened another Firefox browser. I am automatically logged into the same 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 KX II using Firefox and I attempt to log into another KX II using another Firefox browser session from the same client. I am logged off of both KX IIs;. Is this correct behavior?

Yes, to access two different 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

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

U.S./Canada/Latin America

Monday - Friday
8 a.m. - 6 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: +81-3-3523-5991
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
Phone +44(0)20-7090-1390

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. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

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: support.apac@raritan.com