Release Notes for Dominion® KSX II Software Version 2.7

Version: 1.0
Date: February 20, 2016

Applicability: Dominion KSX II models DKSX2-144 & DKSX2-188

Release Status: General Availability.

Dominion KSX II Overview:

Dominion KSX II is Raritan's family of next-generation, secure digital devices that provide an integrated solution for remote KVM (keyboard, video, mouse) server access, serial device management, power control and virtual media from anytime, anywhere from a Web browser.

Release 2.7 Overview:

Release 2.7 is a firmware release, based on Release 2.6, with enhancements, improvements and fixes.

Dominion KSX Release 2.7 Features:

1. Support **View Only Permission** when under CommandCenter management.
2. **Change Default KVM Client to AKC on Windows**. On Microsoft Windows platforms, the Java-free Active KVM Client (AKC) will be launched by default if the environment supports this .NET-based KVM Client. AKC is now available for the Microsoft Internet Explorer and Edge browsers, as well as Chrome with the appropriate plugin. If the Java-based VKC KVM client is desired, then use <IP Address>/vkc or <IP Address>/vkcs with the Chrome or Edge browsers.
3. Support for **Microsoft Windows 10 and Edge browsers**.
4. **Support Chrome Browser (Java Webstart).** The Chrome browser has recently stopped support for the protocol used to launch Java Applets like the Raritan Virtual KVM Client (VKC). This release will utilize Java Webstart to enable the latest Chrome releases (45+) to launch VKC (must use <IP Address>/vkcs).
5. **Support AKC with Chrome**. The Raritan Active KVM Client (AKC), which does not use Java, can be launched via the Chrome browser on Windows platform. This requires the use of the Chrome ClickOnce plugin.
6. **Security enhancements.** Support SHA-2 certificates, new Raritan code signing certificate, update OpenSSL library, increase key size for certificate generation to 4096 bits, the favorites applet only available after login, and stop support for insecure RC4 encryption.
7. Various fixes, small enhancements and documentation updates
8. **KSX II User Guide and Client Guide updates.** The Release 2.7 version of the User Guide is available from the "Help – Online Help" link in the left panel of the KSX II web based user interface and on raritan.com.

Release 2.7 Compatibility Information:

1. **The Dominion KSX II models (KSX2-144 and KSX2-188) and Release 2.7 have been certified for use with CommandCenter® Secure Gateway (CC-SG) Release 6.0 and 6.1.** Customers running previous CC-SG Releases must upgrade to CC-SG 6.0 or later release.

2. KSX II devices can be remotely accessed by four remote clients:

Remote Client	Description
Virtual KVM Client (VKC)	Java-based client invoked from the browser-based remote user interface, for KVM connection to target server. Can force launch by <IP Address>/vkc Use <IP Address>/vkcs on Chrome & Edge
Raritan Serial Console (RSC)	Java-based client invoked from the browser-based remote user interface, for serial port connection to target server.
Multi-Platform Client (MPC)	Java-based MPC with traditional Raritan user interface.
Active KVM Client (AKC)	Windows-based client invoked from the browser-based remote user interface. Can force launch by <IP Address>/akc

3. SUN Java™ Runtime Environment (JRE) version 8 is supported up to 1.8.0_66. SUN Java™ Runtime Environment (JRE) version 7 is supported up to 1.7.0_80. These were the current Java versions at release time. Future Java versions should work correctly assuming no incompatible changes are made. For any issues, please contact Tech Support who can provide workaround solutions or patch releases, if available.
   - Java version 6 is not supported by the Dominion KSX II
   - For best results, we recommend that Java Plug-in Caching is not enabled.
   - For greater security and fewer Java and browser warning messages, Raritan recommends customers upload a SSL certificate to each KSX II switch.
   - Customers need to affirmatively click through all security warnings for the Raritan Java applets to load

4. Internet Explorer versions 10 /11 and the Edge browser are supported. Firefox versions include 33, 38, 40, and 41. Chrome versions 40, 44 and 45. Safari 7.0.5 & 8.0.7.

5. The Active KVM Client (AKC), the native Windows Client, requires Internet Explorer 10 or above and Microsoft .NET Framework versions: 4.0 or 4.5.
   - Windows Vista and Windows 7/8/10 desktops are supported.

6. The above JRE version information applies to the Dominion KSX II when used standalone. When used with CC-SG, please consult the CC-SG Release Notes and Compatibility Matrix.

Release 2.7 Important Notes and Information:

1. **Java Recommendations**. Raritan recommends customers upload a SSL certificate to each KSX II switch. This will eliminate certain Java messages.
2. VKC Direct Port Access with Chrome. Direct Port Access with the VKC KVM Client does not work with Chrome in this release. Please use another browser or AKC if on a Microsoft Windows platform.

Dominion KSX II Documentation:

The following user documentation is available for the Dominion KSX II:

- **Dominion KSX II User Guide** – user guide to the KSX II's local and remote browser based user interfaces and general KSX II usage.
- **Dominion KSX II Quick Setup Guide** –reference for the initial setup of the KSX II.
- **KVM and Serial Client Access Guide** – reference for the remote clients for the Raritan products
- **Dominion KX II CIM Guide** – reference for the Dominion KX II and KSX II Computer Interface Modules (CIMs). Which CIM to use, etc.
- **Dominion KX II Blade Configuration Guide** –contains detailed instructions and screenshots for Dell and IBM blade servers.

The Dominion KSX II documentation is available from the KSX II web based user interface and on the Raritan.com website: www.raritan.com. Please go to the **Support** section and select **Dominion KSX II**. The documentation is shown by release.

Dominion KSX II Online Help:

An **Online Help System** is available. Click on **Help – Online Help** in the left hand information panel. You can browse to the appropriate topic via the Contents, Index and Search tabs. Online help for the Raritan products is available on raritan.com:

http://www.raritan.com/support/online-help/

Computer Interface Module (CIM) Overview:

Dominion KSX II can use the following CIMs:

- **Digital CIMs (D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI, D2CIM-DVUSB-DP):** Customers with servers, PC's or MAC's using the DVI-D, HDMI, or DisplayPort digital video formats should use one of the new digital CIMs. These CIMs will support the KSX standard video resolutions of up to 1920x1080, including widescreen formats.
- **D2CIM-*D*VUSB**: *dual* USB virtual media CIM, required for the virtual media and absolute mouse synchronization features. This CIM is recommended for customers planning to access virtual media drives at the OS and BIOS levels and **for Smart Card and CAC usage**. This CIM requires KSX II Release 2.3 or later. Smart Card feature requires CIM firmware version 3A6E or greater.
- **D2CIM-VUSB**: *single* USB virtual media CIM, required for the virtual media and absolute mouse synchronization features. This CIM is recommended for customers planning to access virtual media drives only at the OS level.
- **KX I DCIMs**: DCIM-PS2, DCIM-USBG2, and DCIM-SUN.
- **DCIM-USBG2**: the DCIM-USBG2 is the recommended basic USB CIM for KSX II. There is a small switch on the DCIM-USBG2, which should be set to the "S" position for use with SUN servers with USB ports.
- **Select Paragon CIMS**: P2CIM-AUSB, P2CIM-PS2, P2CIM-USB, P2CIM-SUSB, P2CIM-SUN, UKVMPD, UUSBPD, UKVM and USKVMPD.
- **Paragon Dual CIMS**: the P2CIM-APS2DUAL and P2CIM-AUSBDUAL are supported.

Firmware Upgrades:

Raritan provides new firmware upgrade releases that contain software enhancements, new features, and improvements. These upgrades are available on www.raritan.com. Please go to the Support section and click on Dominion KSX II or go directly to:

http://www.raritan.com/support/Dominion-ksx-II/

Locate the entry for the new firmware release. Follow the Release Notes to upgrade the device.

Firmware Upgrade Prerequisites:

If you have any questions, or do not meet the pre-requisites listed below, please STOP and contact Raritan Technical Support for further instructions.

General Upgrade Instructions (standalone upgrade from the browser based user interface):

1. **Note: for best results, the KSX II device should be re-booted before the firmware upgrade is applied.** This will ensure no users are logged in or sessions active.

2. The user upgrading the KSX II device must be a member of the default Admin Group to have sufficient administrator-level privileges to update the Dominion KSX II unit.

3. Twenty minutes or more are required for the complete update procedure. The update and subsequent reboot time will vary according to the number and type of CIMs connected to the KSX II.

4. The system provides an estimated time for the firmware upgrade to complete. It may possibly take more time to do the update based on networking conditions and other factors.

5. We recommend backing up the KSX II using the “Backup / Restore” function on the Maintenance menu on the Remote Console before starting the upgrade..

6. Close any remote or local KSX II sessions to all devices connected to the Dominion KSX II unit – servers, power strips, and serial devices.

7. If doing the firmware upgrade over a VPN, ensure that the connection is stable and that no inactivity timeouts have been set.

8. The detailed, step-by-step instructions to perform the upgrade are given below.

9. The software upgrades are written to flash memory, and this takes time to complete. Please do not power-off the unit, or disconnect the Ethernet connection while the upgrade is going on.

10. The KSX II firmware can be upgraded by CC-SG; consult the CC-SG documentation for more information.

11. Should you experience any difficulties with the upgrade, call Raritan Technical Support for assistance.

Step-by-Step Upgrade Instructions:

1. **Note: for best results, the KSX II device should be re-booted before the upgrade**.

2. In the browser, type in the IP Address of your Dominion KSX II unit.

3. Logon as an administrative user “admin” (or other member of the Admin Group).

4. Click on the “Firmware Upgrade” command on the “Maintenance” menu.

5. Browse to locate the .rfp file containing the update. Click the “Upload” button. The current and future versions will be displayed. Click the “Upgrade” button to start the upgrade.

6. The firmware upgrade will then proceed:

   a. You cannot operate the KSX II during the upgrade.

   b. The upgrade panel will inform you of the progress of the upgrade. This upgrade step will take up to 15 minutes or more.

   DO NOT REBOOT OR POWER CYCLE THE KSX II DURING THE UPGRADE OR THE REBOOT!

   c. You will see a completion message when the upgrade completes.

7. The device will now reboot and reset, which may take up to 5 minutes.

8. Close your web browser session and log back in after the reboot completes.

9. The KSX II will beep when complete and the login screen will appear on the local console.

10. Log back in via web browser or the local port. Use the “Upgrade History” report” on the “Maintenance” menu to check the upgrade status.

11. Any KSX II CIMs connected to the KSX II will be upgraded also.

If you have any questions or issues during the update, call Raritan Technical Support.

Release 2.5 Important Notes and Information for Digital Video CIMs:

1. The Digital Video CIMs support E-EDID and DDC to communicate the "Preferred Timing Mode," i.e. the user's preferred video resolution, as well as the other supported video resolutions, to the target server. This preferred video resolution, known as the "Display Native Resolution" on the Port Configuration page on the LX user interface, defaults to 1280x1024@60hz, but can be changed by the user.
2. Some servers, especially at the BIOS level, may not automatically change to the preferred (native) resolution provided by the CIM to the server. Users can manually change the "Display Native Resolution," change the resolution manually on the server, re-boot the server or consult the server or LX documentation for additional suggestions.
3. Sometimes video may not display for certain preferred video resolutions on some servers. Try using a different resolution, re-boot the server or consult the server or LX documentation.
4. Do not change the port's "Display Native Resolution" during virtual media transfers – it may interrupt the transfer.
5. On Linux, you may need to restart the X window system or reboot the system when changing the "Display Native Resolution."
6. DVI-D and DVI-I are supported by the D2CIM-DVUSB-DVI, but not DVI-A (less common).
7. The D2CIM-DVUSB-HDMI CIM does not support HDCP or embedded audio. For some servers, the "DVI Compatibility Mode," which provides a DVI compatible video signal, will provide improved video quality. This can be set on the Port Configuration page.
8. The D2CIM-DVUSB-DP does not support DPCP or embedded audio.

Release 2.3.5 Important Notes and Information:

1. Dominion KSX II Tiering (Cascading) - is <u>not</u> available in this release
2. Hot-Key Based Generic KVM Tiering - is <u>not</u> available in this release.
3. Our support of 1920x1080 HD Video Resolution is via standard VGA (analog) video. Servers with DVI-A (analog) and DVI-I (integrated analog and digital) ports can use the new Raritan ADVI-VGA adapter to convert the DVI signal to VGA.
4. Paragon II Dual CIMS (P2CIM-APS2DUAL and P2CIM-AUSBDUAL):
   - The Paragon Dual CIMs are basic CIMs, so advanced features such as: Virtual Media, Smart Card, Absolute Mouse Mode, blade servers, tiering are not supported.
   - You must configure both KSX II's for either Private Mode -or- PC-Share Mode
   - The KSX II user group level PC-share permissions are not supported with these CIMs.
   - Note that CIM name changes are not updated on the other KSX II switch until that switch attempts to connect to that port. Port status changes are handled similarly.
   - You can connect a dual CIM to a KSX II and Paragon simultaneously, but then you must configure them both for Private or PC-Share modes.

   - The Paragon II Public View Mode is not supported.

5. IPv6 is not supported for AKC Client. Use one of the Java Clients (VKC, MPC) instead.
6. In fall of 2010, new hardware versions of the D2CIM-VUSB and D2CIM-DVUSB were released. These CIMs have a new hardware version: D2CIM-[D]VUSBG2-AA and new firmware versions:
   - 4Axx for the new D2CIM-VUSB
   - 5Axx for the new D2CIM-DVUSB
7. Power associations will remain even if a new rack PDU (PX) is plugged into the KSX II. If new associations are required, then these must be manually changed.

Release 2.2 Important Notes and Information:

Note that KSX Release 2.7 contains features from Dominion KSX II release 2.2. The following describes notes and information for those features.

1. Microsoft's Internet Explorer (IE6 and above) must be used to launch AKC. Windows XP, Vista and Windows 7 user desktops are supported. Microsoft's .NET Framework 3.5 is required.
2. AKC can be launched from IE using HTTPS or HTTP with the following syntax: http[s]://<KSX II IP Address>/akc/

   The "Enable AKC Download Server Certificate Validation" check box on the "Device Settings" page controls how AKC is launched by IE.

   If disabled (default), users must ensure that (1) cookies from the IP address of the KSXII device being accessed are not currently being blocked, and (2) Vista, Win 7, Win 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.

   If enabled, then the administrator must upload a SSL certificate with a valid host designation for the KSX II. In addition the user must add the certificate to the browser's Trusted Root CA store.

   CommandCenter has the same checkbox and similar operation to launch AKC.

   If AKC is minimized when it is closed, it will be minimized when launched.
3. IPv6 is not yet supported by AKC.
4. If the "Enable FIPS Mode" checkbox on the "Security Settings" page is enabled, the KSX II switch must be re-booted to enter FIPS mode and use the Validated FIPS 140-2 Cryptographic Module. When in FIPS mode, the left hand information panel displays this mode, RC4 encryption is disallowed and KVM & virtual media encryption is enforced.
5. For FIPS compliant operation, each KSX II switch requires a SSL certificate created in FIPS mode. This can be done by creating a new SSL certificate in the "Certificate Settings" page.
6. Several Virtual Media options are now available for users without administrator permission in AKC.

7. To use the enhanced Apple MAC BIOS entry, the D2CIM-VUSB or D2CIM-DVUSB CIM firmware must be updated. Ensure the CIMs are attached when the KSX II is upgraded to Release 2.2. Also a MAC specific USB profile should be used: BIOS Mac USB profile or Mac OS-X (10.4.9 and later) USB profile.
8. On Windows 7 target servers, mounted virtual media drives may not be visible in the "My Computer" folder, due to a new Windows 7 feature. To disable it, go to "Folder options"->"View" and uncheck "Hide empty drives in the Computer folder".
9. On Windows 7, with User Account Control (UAC) on, if not "Running as Administrator' in IE, the user will not have access to all Virtual Media Resources, in particular fixed drives and fixed drive partitions.
10. For certain servers, particular widescreen formats may not be available when the KSX II CIM is attached. If so, disconnect the CIM, set the resolution and re-connect the CIM. Alternatively, the following Raritan adapters can be used: DDC-1440 and DDC-1680.
11. When using Direct Port Access with the new AKC Windows client, after connecting to the first target server port, a new browser window or tab should be used for subsequent connections.

Release 2.1.10 (Smart Card) Important Notes and Information:

Note that KSX Release 2.7 contains features from Dominion KX II Release 2.1.10. The following describes notes and information for those features.

1. **The D2CIM-DVUSB must be connected to target servers requiring Smart Card / CAC authentication.** The DVUSB CIM must have firmware version 3A6E or greater loaded on it. It will be upgraded if it is connected to the Dominion KSX II switch when it is upgraded to Release 2.3 or later. Otherwise upgrade it separately.
2. The Smart Card feature requires Java Runtime Environment 1.6.x with the SmartCard API. The Smart Card feature also requires a PC/SC compliant computing environment on the client PC and a standard USB CCID device driver on the target server. Supported transmission protocols supported (used by the smart card) are T=0 and T=1. For more information, see the "Minimum System Requirements" in the "Smart Card Readers" section in Appendix A of the Dominion KSX II User Guide.
3. For a list of tested and certified Smart Card Readers, see "Supported and Unsupported Smart Card Readers" in the "Smart Card Readers" section in Appendix A of the Dominion KSX II User Guide.
4. VKC and MPC are supported for Smart Card/CAC authentication on Windows client platforms. Apple MAC and SUN Solaris clients do not support Smart Card / CAC authentication. Certain Linux versions are supported – see below.
5. Linux Clients. Only the following Linux operating systems are certified for use as remote clients supporting Smart Card/CAC authentication with the required PC/SC library versions:

	Smart Card Requirement
Operating System	**PC/SC**
Red Hat Enterprise Linux 5 (RHEL 5)	pcsc-lite-1.4.4-0.1.el5 pcsc-lite-libs-1.4.4-0.1.el5
SUSE 11	version 1.4.102-1.24

Fedora Core 10	pcsc-lite-1.4.102.3.fc10.i386 pcsc-lite-libs-1.4.102-3.fc10.i386

6. Linux Target Servers. To support Smart Card / CAC authentication for Linux servers in the data center, a new open-source card reader driver is required. This driver is not yet available in current LINUX distributions. For more information, see the “Minimum System Requirements” in the “Smart Card Readers” section in Appendix A of the Dominion KSX II User Guide and contact Raritan Technical Support. In addition, the following CCID driver versions are required:

	Smart Card Requirement
Operating System	**CCID**
RHEL 5	ccid-1.3.8-1.el5
SuSE 11	CCID 1.3.8-3.12
Fedora Core 10	CCID 1.3.8-1.fc10.i386

7. KSX II front-end to Paragon II. Smart Card and Virtual Media are not supported when using Dominion KSX II as a front-end to Paragon II. When first accessing the Paragon II OSD through KSX II, do not synchronize the mouse manually. A mouse is not needed and may delay the keyboard response for several seconds.
8. The supported distance from KSX II to the Paragon II user station is up to 150 cable feet (45 m). The supported distance from the Paragon II user station to the target server is up to 500 cable feet (152 m). Greater distances may result in video degradation.

Release 2.1 (Blade Server) Important Notes and Information:

Note that KSX Release 2.7 contains features from Dominion KSX II release 2.1. The following describes notes and information for those features.

1. Blade server support is dependent on the particular blade server manufacturer and model. In general, there are two types: (1) connect a CIM to each blade and (2) connect a CIM to the blade server chassis’ internal KVM switch or management module. The module must be configured to work with the KSX II. Consult the documentation or technical support for instructions. The Dominion KX II Blade Configuration guide contains detailed instructions and screenshots for Dell and IBM blade servers.
2. When connecting to individual Dell 1855/1995 blades, the “USB Front Dongle for Dell PowerEdge 1855/1955” cable is required; manufacturer part number N8138 and Dell part number 310-6484. For HP c3000 and c7000, the “HP c-Class Blade SUV Cable” is used; part # is 416003-001. Use the Port Group Management feature to group the ports. Note: the internal KVM module for the HP c3000 is not supported in this release.
3. Paragon blade server CIMs are not used with the Dominion KSX II. Use the appropriate KSX II CIM according to the type of ports on the blade server (PS2 or USB) and whether the advanced features (e.g. virtual media) are wanted and supported. See the Dominion KX II CIM Guide for more information.
4. Virtual media and advanced mouse synchronization is supported on blade servers where a CIM is connected to each blade, assuming the operating system on the blade supports it. Virtual media is also supported on the IBM Blade Center E and H chassis when using the D2CIM-DVUSB connected to the front and rear of the chassis, with auto-discovery enabled.

5. For blade server chassis with internal KVM switches, for performance and reliability reasons, there is a limit of 8 blade servers per KSX II. If you connect a CIM to each individual blade server, then there is no limit.
6. For the IBM BladeCenter, the Advanced Management Module (AMM) is supported. The older Management Module has not been certified in this release. The KSX II only supports auto-discovery for AMM[1] as the acting primary management module.
7. The following IBM BladeCenter minimum AMM firmware is recommended:

   Management Module Firmware
   Main application: BPET36K
   Released: 04-22-08
   Name: CNETMNUS.PKT
   Rev: 54

8. When connecting to a blade server in the IBM BladeCenter, you should wait a few seconds after seeing the video before moving the mouse. If not, then the mouse may be out of synch and you should manually synchronize it.
9. In a CC-SG environment, once a blade chassis type port has been configured on the KSX II, the blade chassis should not be moved to another port.
10. The blade server feature is not currently supported by the Dominion KX II-101 product.
11. When blade chassis type ports are connected to the KSX II, the User Management Group page must be edited remotely, rather than from the local port.
12. CC-SG 5.1 (or later) is required for use with the blade server feature.
13. Contact the Dominion KSX II documentation, CIM Guide and Blade Configuration Guide or technical support for more information.

Release 2.0.X Important Notes and Information:

Note that KSX Release 2.7 contains features from Dominion KSX II releases 2.0.x. The following describes notes and information for those features.

1. For reliable network communication, configure the KSX II and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the KSX II and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.
2. There are several prerequisites for Virtual Media: (1) a D2CIM-VUSB or D2CIM-DVUSB must be connected to the server's USB port, (2) the operating system (OS) or BIOS must support USB connected devices, and (3) the user must have the required administrator permissions on the client, target and the KSX II.
3. Not all servers and operating systems support all virtual media options. In general, modern Windows® OS' do, including Windows Vista™, 2003 Server, XP and Windows 2000 with the latest patches. Target Servers running Linux and Mac OS', when accessed from a Windows client, will generally mount CD/DVD drives, USB drives and ISO images. Mac®, Linux and Solaris™ clients can only mount ISO images from a local or remote drive. Other UNIX based OS' generally do not support virtual media.

4. In general, due to varying BIOS implementations of the USB 2.0 standard regarding virtual media, it is not always possible to boot from a virtual media drive at the BIOS level. **The D2CIM-DVUSB CIM is recommended for customers who plan to use virtual media at the OS and BIOS levels.** Use D2CIM-VUSB for virtual media at the OS level and for the BIOS level when supported by the particular BIOS or with an applicable BIOS USB profile. Please note that some BIOS do not support USB devices as boot devices and hence virtual media is not possible.
5. For Windows OS', do not use the "Safely Remove Hardware" function in the system tray on the target server to disconnect a mounted virtual media drive. Disconnect using the "Disconnect" command on the virtual media menu.
6. Absolute Mouse Synchronization requires support from the OS. Windows and Mac OS' generally support it. Linux and UNIX based OS' (AIX, HP-UX, Solaris) generally do not.
7. When a panel is opened in the Virtual KVM Client (VKC), the client, as well as related browser tabs and windows, will wait for user input until the panel is closed.
8. Be careful of the web browser refresh or reload function/button, which has the side-effect of closing VKC sessions.
9. To use AES encryption, first ensure that your web browser supports this stronger encryption – not all browsers do. For AES, set the "Encryption mode" on the "Security Settings" panel to "AES," not "Auto" which generally results in RC4 encryption. 128 bit and 256 bit AES encryption are supported.
10. For the best possible video quality, adhere to these distance guidelines from the CIM to the KSX II:

Server Video Resolution	Distance
1024x768 (and below)	150 feet
1280x1024	100 feet
1600x1200	50 feet

11. To further minimize network bandwidth for lower bandwidth situations, set the "Noise Filter" on the "Video Settings" panel in the remote clients above the default value of 2 - values of 3 or 4 are recommended.
12. In general, most administrative functions are available on the remote and local consoles. But some functions, by their nature, are only available on one console. For example, "Factory Reset" is only available on the local port. Firmware Update, Backup and Restore, and certain KSX II Device Diagnostics features are available from the remote client.
13. IPv6 usage notes. IPv4 networking is the factory default. Enable IPv6 on the Network Settings panel for IPv6/IPv4 "dual stack" operation. IPv6 is available in standalone configuration. Access of remote ISO images in a virtual media connection via IPv6 is not supported due to third party software limitations. IPv6 with Apple MAC OS Leopard is not supported.

    The Standalone Multi-Platform Client, available in the firmware section of raritan.com, must be used for modem connections. In order to enhance performance, modem connections are established with 4 bit grey and 33 Kbps connection parameters. Firmware upgrade over a modem connection is not supported. Modem sessions not currently supported from Apple MAC and Linux clients. Consult the User Guide for more information.

14. When changing the various user management, device and security settings, please remember to click the "OK" button at the end of the page to save and activate your changes.
15. SUN Backgrounds: Some of the SUN background screens may not center precisely on certain SUN servers, i.e. those backgrounds with dark borders (e.g. NoBackDrop). Use another background or place a light colored icon in the upper left hand corner.
16. An apostrophe (') is no longer an allowed character for port (CIM) names.
17. For Mac OS, the Safari™ browser is certified for use. Absolute Mouse Synchronization is required for Mac servers. The "Mac OS-X (10.4.9 and later)" USB profile should be enabled for the specific port on the Port Configurations page.

KSX Release 2.0.X Important Notes and Information:

1. When using CC-SG, the power ports should be inactive before attaching power strips that were swapped between the power ports. If not, there is a possibility that the number of power outlets will not be correctly detected, especially after swapping 8 and 20 outlet power strip models.
2. The username should not contain the ' \' character.
3. When running the Multi-Platform Client (MPC) the Serial Connection menu options are displayed even though they may not be applicable.
4. The Command Line Interface does not support the Delete key, the Backspace should be used instead.
5. Mouse synchronization does not converge completely with IBM AIX target servers.
6. The stand alone Raritan Serial Console (RSC) is not supported on MAC OS X.
7. The minimum acceptable length for 'weak' passwords is 4 characters.
8. If 'Apply Encryption Mode to KVM and Virtual Media' is disabled, encryption mode settings are applied as requested by client browser.
9. Entry of keyword(s) in an invalid format will require re-entry of the keyword set.
10. Executing a 'Restore' will cause a system reboot in order to apply changes.
11. MS-DOS applications running in windows on serial targets may require key mappings not currently supported (ALT).