Dominion KSX II Release 2.5

February 21, 2013

Table of Contents

Release Notes for Dominion® KSX II Software Version 2.5

Version: DKSX II 2.5 Release Notes, Revision 1.0
Date: February 21, 2013

Effective:

Immediately.

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 2.5 Overview:

KSX Release 2.5 is a new feature release, based on features from Dominion KX II Releases 2.4 and 2.5. With this Release, KSX supports the new Digital CIMs that support servers and PC's with DVI, HDMI and DisplayPort video.

Dominion KSX Release 2.5 Features:

1. **Support for New Digital Video CIMs.** Servers with DVI, HDMI and DisplayPort video are supported via the D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI & D2CIM-DVUSB-DP digital video CIMs.
2. **Mobile KVM Client.** Mobile KVM access for iPhone and iPad. Users can now access and control servers connected to the Dominion KX II via their Apple iPhones and iPads. This provides emergency 24x7 out-of-hours access, as well as convenient everyday access for iPad enthusiasts. CC-SG Release 5.2 or later is required for this capability.
3. **Display and Logoff Users by Port.** Users can view a list of connected users by port, and Administrators can logoff users by port or completely. Supports locally and remotely (LDAP, Radius, etc.) authenticated users.
4. **CC-SG Management with IPv6.** Interoperates with CC-SG using IPv6.
5. **SNMPv3.** This more secure version of SNMP is now supported.
6. **Auto Scan and Thumbnail Views.** View selected servers as a slide show and via thumbnail views. See real time updates of server video. The user can select a list of servers, set the scan interval and quickly access a given server. Works remotely and locally.
7. **Asian Languages – Japanese and Simplified/Traditional Chinese.** The Dominion KX II's remote HTML User Interface and the KVM Clients now support the Japanese, Simplified

Chinese and Traditional Chinese languages. This is available standalone as well as through CC-SG.

8. **Connect/Disconnect Scripts.** Customers can define scripts that are executed when the user connects to or disconnects from a remote server. This is useful to wake up a server, launch the login screen and/or automatically log off.
9. **Edit Unconnected Port Names.** Can now name or reset a KX II port that does not have a CIM connected to it.
10. **Vulnerability scanning and security updates**.
11. **Virtual Media for Linux and Mac.** Expands the benefits of virtual media to Linux and Mac clients. Previously, Mac and Linux clients could only mount ISO images from a local drive or remote server. Now Linux and Mac Clients can now mount USB drives, PC hard drives, CDs, DVDs and ISO images.
12. **Apple MAC Snow Leopard and Lion Server BIOS startup and function keys.** Support for various (Option, Command and other) keystrokes used during BIOS startup.
13. **USB Profile Improvements.** Three additional Profiles added. Capability to change active profile directly from the KVM Clients.
14. **OpenSSL Version 1.2.4.** Incorporated this new security module for updated FIPS 140-2 security.
15. **KSX II User Guide and Client Guide updates**. The Release 2.5 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.

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**: new for Release 2.3, the P2CIM-APS2DUAL and P2CIM-AUSBDUAL are now supported.

Release 2.5 Compatibility Information:

1. **The Dominion KSX II models (KSX2-144 and KSX2-188) and Release 2.5 have been certified for use with CommandCenter® Secure Gateway (CC-SG) Release 5.3.** Customers running previous CC-SG Releases must upgrade to CC-SG 5.3 or later release.

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

Remote Client	Description	Version
Virtual KVM Client (VKC)	Java-based client invoked from the browser-based remote user interface, for KVM connection to target server.	Version 3.0.2
Raritan Serial Console	Java-based client invoked from the browser-based remote user interface, for serial port connection to target server.	RSC 3.0.0
Multi-Platform Client (MPC)	Java-based MPC with traditional Raritan user interface.	MPC 7.0.2
Active KVM Client (AKC)	Windows-based client invoked from the browser-based remote user interface.	AKC 1.0.5

3. **SUN Java™ Runtime Environment (JRE) version 1.6 is now the minimum version.** JRE 1.7 (Java 7) is also supported. The certified JRE builds are JRE 1.6.0_24 through 1.7.0_11.
4. For best results, we recommend that Java Plug-in Caching is not enabled.
5. SUN Java™ Runtime Environment (JRE) versions 1.4.x and 1.5.x are not 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.
7. Due to browser/Java compatibility issues with Apple Mac OS 10.4/10.5, JRE 1.6 and Raritan's Java based KVM clients (MPC, VKC), we recommend the following for customers on Apple Mac desktops (when the KVM Client is used there):
   a. **Mac OS 10.4**: remain with KSX II Release 1.0.x or upgrade to Mac OS 10.6
   b. **Mac OS 10.5/Power PC**: remain with KSX II Release 1.0.x or upgrade to Mac OS 10.6
   c. **Mac OS 10.5/Intel**: remain with KSX II Release 1.0.x, upgrade to Mac OS 10.6 or install the standalone version of MPC on Mac OS 10.5
   d. **Mac OS 10.6**: fully supported with Java 1.6
8. If the client does not have a JRE associated with the Browser or if the JRE version is below 1.6, then a message will be displayed, and the user will be directed to install the latest version from the SUN Java website.
9. The JRE installation requires the multi language option to be enabled for Korean and other non-English language support. For a "Custom" JRE installation, must ensure that "Support for Additional Languages" is included during the installation process.

10. AKC requires the use of Internet Explorer 6 or above and Microsoft .NET Framework 3.5 or higher. Use a URL of the form: http[s]://<KSX II address>/akc/. Windows XP, Vista and Windows 7 desktops are supported.

    AKC requires Microsoft .NET Framework version 3.5 and Internet Explorer 8 or 9.

11. Java is required even if AKC is used. The reason for this is that the Raritan Serial Client requires the Java Runtime Environment.
12. Internet Explorer 8 & 9 are supported. IE 6 is no longer supported. Supported Firefox versions are: 10, 12, 16.0.2 and 17. We recommend Safari version 6.0.2.
13. The following, legacy operating systems are no longer officially supported as target servers: Solaris 9, Fedora all versions before 13, SUSE all versions before 10.x. Consult the User Guide for more information.
14. Use the pre-defined macros created for the Japanese Kana Key and the R-ALT-KANA key, as these keys are not consistently received from the JRE.
15. There is a new SNMP v2 MIB. This should be loaded into your SNMP management system if you are enabling SNMP traps from your KSX II switch.

64 Bit Windows Client Support: Java Requirements

The following 64 bit Windows clients are supported: Windows 7 (64 bit), Windows XP Professional 64-bit, Windows Vista 64-bit, and Windows Server 2008 64 bit.

For the Virtual KVM Client and Multi-Platform Client when accessed as Java applets – i.e. from the KSX II HTML user interface or through CC-SG, the following is important:

1. Both the 32-bit and 64 bit JRE plug-ins are supported.
2. The 32 JRE plug-in has been certified with the following 32 bit browsers: Firefox 3.0, Internet Explorer 7 and Internet Explorer 8.
3. The 64 bit plug-in has been certified with Internet Explorer 7 and Internet Explorer 8.
4. For the standalone version of MPC, either a 32-bit or 64-bit JRE plug-in can be used.

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, go to **Firmware and Documentation** and then select **Dominion KSX II**. The documentation is shown by release, so click on the appropriate release.

Dominion KSX II Online Help:

An **Online Help System** is available. Click on **Help – Online Help** in the left hand information panel and the Online Help system will launch. You can browse to the appropriate topic via the Contents, Index and Search tabs. The entire Dominion KSX II User guide is available, including text and images, with an extensive set of links. Online help for the Raritan products is now available on raritan.com:

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

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.

Dominion KSX Release 2.3.5 (Previous Release) Features:

1. **The D2CIM-DVUSB is a dual USB virtual media CIM, recommended for customers planning to use virtual media drives at the BIOS level.** This CIM has two USB plugs: one for keyboard/mouse and one for virtual media drives. This CIM is recommended for customers planning to use virtual media drives at the BIOS level, since some BIOS have difficulty supporting keyboard, mouse and virtual media on a single USB plug. Also required for Smart Card use.
2. **Blade Server Support for Dell, HP and IBM Blade Servers.** KSX II based local and remote access of Dell, HP and IBM blade servers. Available standalone and thru CC-SG Release 5.1.
3. **Smart Card and Common Access Card (CAC) Target Server Authentication**. Smart Card and Department of Defense Common Access Card (CAC) authentication from the remote clients to the target server. With this feature, the user can remotely log on to the target server in the data center using a Smart Card connected to their remote workstation. This is supported at-the-rack, standalone over IP and through CC-SG. Meets U.S. Government HSPD-12, PIV and CAC directives and ISO 7816, PC/SC and CCID standards. All Dominion KSX II models support Smart Cards using the D2CIM-DVUSB CIM.
4. **Windows-Based Active KVM Client (AKC).** A new, native Windows KVM Client is now available for use with CC-SG as well as standalone. This client does not use Java.
5. **Validated FIPS 140-2 Cryptographic Module.** The Dominion KSX II, as of Release 2.3, uses 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. FIPS cryptography is supported for KVM sessions and also for serial sessions when the Raritan RSC client is used.
6. **Dual Stack IPv6 and IPv4 Networking.** The Dominion KSX II provides "dual stack" IP networking with simultaneous support of IPv4 and IPv6. Relevant KSX II features enhanced to support IPv6. Support for IPv6 network settings and IPv6 addressable external servers, i.e. SNMP, LDAP, etc. Discovery of IPv6 devices.
7. **256 Bit Advanced Encryption Standard (AES).** The Dominion KSX II now supports 256 bit AES encryption for SSL connections. This option can be enabled on the "Security Settings" page.
8. **HD Video - 1920x1080 Resolution**. The Dominion KSX II now supports full High Definition (HD) 1920x1080 @ 60 hz remote video resolution. Note this is VGA (analog) video. For target servers with DVI-I or DVI-A video, the new Raritan ADVI-VGA adapter can be used.
9. **Widescreen Resolutions.** Support widescreen video resolutions including: 1280x720@60, 1366x768@60, 1440x900@60 and 1680x1050@60.
10. **Dual/Multi Monitor KVM Client Support**. Support for multiple LCD monitors; the KSX II can launch KVM sessions to multiple monitors, either in full-screen or standard modes. In this mode, users can view the list of servers on one screen and launch full-screen KVM sessions in another. Or use a secondary, desktop monitor exclusively for KVM.
11. **Launch in Full Screen Mode (hidden toolbar)**. The KVM clients can be configured to launch KVM sessions in full screen mode. With a new hidden menu bar, users can run KVM client functions while in full-screen mode. This toolbar remains hidden, until the user moves the mouse cursor to the top of the screen.

12. **Super Speedy Single Mouse Performance**. The performance of single mouse mode has been improved. Single mouse mode requires no mouse synchronization on the target server.
13. **Send Text to Target Server feature.** This feature will send user text from the remote KVM clients to an application on the target server.
14. **The USB Profile feature** customizes the Dominion KSX's keyboard, mouse and virtual media USB interface for specific target servers, overcoming the limitations and characteristics of the USB implementation of the BIOS or OS. This enables broader support of virtual media devices at the BIOS level as well as supporting the varying mouse synchronization required for Linux and Mac servers.
15. **Virtual media support of 1 to 2 terabyte hard drives**.
16. **Virtual Media options without administrator permission in AKC.** Several forms of virtual media are available in AKC, even without administrator level permissions.
17. **Enhanced Command Center Secure Gateway connectivity management**. Should a Dominion KSX II under CC-SG management lose connectivity with the CC-SG due to loss of network connectivity, then the device will automatically and temporarily become available for standalone access. (Admin users will also have the option to remove the device from CC-SG management). When connectivity is restored, then CC-SG management of the device will be automatically re-established.
18. **Full KSX II Administration Settings from CC-SG.** When launching KSX II from CC-SG's "Launch Admin" function, the full set of administration settings is now available.
19. **CC-SG Proxy Mode Enhancements.** When used with CC-SG Release 5.1, Release 2.5 supports virtual media and SSL encryption in CC-SG's proxy mode.
20. **Device Access While Under CC-SG Management.** Users can now optionally access a KSX II directly even when under CC control.
21. **Customer provided SSL Certificate**. Administrator can create a certificate signing request and upload a customer provided SSL certificate for enhanced security.
22. **Customer Specific Security Banner**. For government, military and other security conscious customers requiring a security message before user login, the KSX II can display a user-configurable banner message and require acceptance before user login.
23. **Configurable Port Numbers (Stealth Mode)**. For customers wishing to increase security by avoiding the standard TCP/IP port numbers, the Dominion KSX II allows the administrator to configure alternate port numbers.
24. **KVM Sessions thru a Proxy Server**. For customers wishing to run KVM sessions over a SOCKS proxy server, we have documented the steps required.
25. **Force Local User Log Off**. Administrators can log off local users.
26. **PX "Strip Level" Statistics.** For PX power strips connected to a KSX II, strip level power statistics and information are provided to the user.
27. **Power cycle by outlet.** The user can power cycle specific power strip outlets without the need to create an association. Useful for non-server devices (turn off the lights)

28. **Keyboard Macro Import/Export.** VKC, MPC and AKC can import and export user defined macros. Macro improvements including Sun keys, delays in macros and an Add button that adds both press and release.
29. **Save Connection Parameters in VKC, MPC, AKC and CC-SG.** Connection properties (Connection Speed, Color Depth and Smoothing) changes are now saved by the remote client software and are now maintained on a per user and Dominion KSX II basis.
30. **LDAP Authentication Enhancements.** Improvements to LDAP authentication including LDAPS Server Certificate Validation options and a new Test LDAP Server Access function.
31. **Microsoft Windows 7 Support.** Support of Microsoft's latest operating system. Windows 7 is supported as a target server as well as a customer desktop.
32. **Direct Port Access via URL**. Single click access to a specific port on the KSX II via a URL.
33. **Paragon Dual CIMs (P2CIM-APS2DUAL and P2CIM-AUSBDUAL)**. The Dominion KSX II now supports Paragon II Dual CIMs, which can connect servers in the data center to two different Dominion KSX II switches. If one KSX II switch is not available, the server can be accessed through the second KSX II switch, providing redundant access and doubling the level of remote KVM access.
34. **Raritan DVI to VGA Adapter**. A Raritan DVI to VGA adapter (ADVI-VGA) is available. This will convert DVI-I/DVI-A server ports to VGA for use with VGA-based Raritan CIMs or cables.

Release 2.3.5 Important Notes and Information:

1. Dominion KSX II Tiering (Cascading) - is not available in this release
2. Hot-Key Based Generic KVM Tiering - is not 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 2.5 contains features from Dominion KX 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 2.5 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 2.5 contains features from Dominion KX 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 2.5 contains features from Dominion KX 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 <u>not</u> 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 in KSX Release 2.5. 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).

Firmware Upgrades:

Customers can upgrade Dominion KSX II switches with Release 2.5 to get a new security certificate.

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

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

Locate the entry for the new firmware release. Release Notes are available with: (a) brief descriptions of new features/enhancements, (b) important operating instructions, and (c) firmware upgrade instructions. Follow the Release Notes instructions 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. Please read the entire instructions (this document) before proceeding.

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 firmware upgrade is applied.** This will ensure no users are logged in or sessions active.

2. In Internet Explorer (or other supported web browser), type in the IP Address of your Dominion KSX II unit, and wait as the web based interface loads.

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 the upgrade is complete and the login screen will appear on the local console port.

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 (D2CIM-VUSB, D2CIM-DVUSB) connected to the KSX II at the time of the upgrade will be upgraded also.

12. To support the Smart Card feature, the DVUSB CIM must have firmware version 3A6E (or greater) loaded on it. Use the "CIM Firmware Upgrade" menu on the "Maintenance" menu to check the CIM version(s) and to upgrade any additional D2CIM-DVUSB CIMs inserted after the upgrade.
13. Due to improvements made in subsequent releases, you cannot downgrade (or restore with a backup file) from Release 2.3 or later to Release 2.0.
14. Due to hardware changes in the Dominion KSX II switches, customers should not downgrade switches loaded with Release 2.5 to an earlier release.
15. If you have any questions or issues during the update, call Raritan Technical Support for assistance.