Dominion KX II Release 2.5

June 8, 2012

Table of Contents

Release Notes for Dominion® KX II Software Version 2.5

Version: DKX II 2.5 Release Notes, Revision 1.4

Date: June 8, 2012

Effective: Release 2.5 Firmware available immediately.

Digital CIMs available in June, 2012.

Applicability:

Dominion KX II models:

DKX2-108, DKX2-116, DKX2-132, DKX2-216, DKX2-232, DKX2-416, DKX2-432, DKX2-464, DKX2-808, DKX2-832, DKX-864

Release Status: General Availability.

Dominion KX II Overview:

Dominion KX II is Raritan's next-generation, KVM-over-IP switches with dual power supplies and dual gigabit Ethernet ports. KX II has a new user interface supporting advanced features such as virtual media, absolute mouse synchronization, blade servers, smart cards, audio, iPhone/iPad interface, tiering and 1920x1080 remote video resolution. The Dominion KX II supports both analog and digital video (DVI, HDMI and DisplayPort) through a single KVM-over-IP switch without adapters.

Release 2.5 Overview:

Release 2.5 is a firmware release, based on Release 2.4, with enhancements and improvements. The Release is required to use the new Digital CIMs, available in June 2012, that support DVI, HDMI and DisplayPort video.

Dominion KX Release 2.5 Enhancements:

1. **Support for New Digital Video CIMs**. Servers with DVI, HDMI and DisplayPort video are supported via the new D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI & D2CIM-DVUSB-DP CIMs available in June 2012.
2. **Dual Video Support.** Servers with dual video outputs are now supported. Connect a CIM to each video output, create a port group, configure and remotely access both video ports in an extended desktop.
3. **SNMPv3**. This more secure version of SNMP is now supported.
4. **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.
5. **Audio Enhancements**. Enhancements to the digital audio feature, including support for PC Share and higher fidelity recording.
6. **Apple MAC Snow Leopard and Lion Server BIOS startup and function keys.** Support for various (Option, Command and other) keystrokes used during BIOS startup.
7. **Vulnerability scanning and security updates.**
8. **KX 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 KX II web based user interface and on raritan.com.

Dominion KX II Documentation:

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

Dominion KX II User Guide – user guide to the KX II's local and remote browser based user interfaces and general KX II usage.

Dominion KX II Quick Setup Guide –for the initial setup of the KX 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 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 KX II documentation is available from the KX 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 KX II**. The documentation is shown by release, so click on the appropriate release.

Dominion KX 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 KX 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/

Computer Interface Module (CIM) Overview:

Dominion KX II can use the following CIMs:

D2CIM-*D*VUSB: *dual* USB, VGA-based virtual media CIM, required for virtual media, absolute mouse synchronization, and the advanced KVM features. This CIM is recommended for customers planning to access virtual media drives at the OS/BIOS levels as well as the Smart Card, tiering and audio features.

D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI & D2CIM-DVUSB-DP: New DVI, HDMI and DisplayPort versions of the D2CIM-DVUSB, available in June 2012.

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. The DCIM-USB and DCIM-SUSB are end-of-life, so the DCIM-USBG2 is now recommended.

DCIM-USBG2: the DCIM-USBG2 is the recommended basic USB CIM for KX 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.

D2CIM-PWR: required to connect a remote power strip to the KX II.

Select Paragon CIMS: P2CIM-AUSB, P2CIM-PS2, P2CIM-USB, P2CIM-SUSB, P2CIM-SUN, UKVMPD, UUSBPD, UKVM and USKVMPD.

Paragon Dual CIMS: as of Release 2.3, the P2CIM-APS2DUAL and P2CIM-AUSBDUAL are now supported.

P2CIM-SER, which can be connected to serial devices. When loaded with firmware V2.63 or greater, it is certified for use with KX II switches.

Release 2.5 Compatibility Information:

1. The above Dominion KX II models and Release 2.5 have been certified for use with CommandCenter® Secure Gateway (CC-SG) Releases 5.2 and 5.3. Raritan recommends that customers upgrade to the CC-SG 5.3 or later release, for best results.

2. KX II devices can be remotely accessed by three KVM remote clients:

Remote Client	Description	Version
Virtual KVM Client (VKC)	Java-based client invoked from the browser-based remote user interface. **KX II switches only.**	Version 3.0.1
Multi-Platform Client (MPC)	Java-based MPC with traditional Raritan user interface. **KX I and KX II switches.**	Version 7.0.1
Active KVM Client (AKC)	Windows-based client invoked from the browser-based remote user interface. **KX II switches only.**	Version 1.0.4

3. **SUN Java™ Runtime Environment (JRE) versions 1.4.x and 1.5.x are <u>not</u> supported!**

4. **SUN Java™ Runtime Environment (JRE) versions 1.6 and 1.7 are supported**. The certified JRE builds are JRE 1.6.0_24 through 1.7.0_11, although later versions will generally work.

   For best results, we recommend that Java Plug-in Caching is **<u>not</u>** enabled.

5. Internet Explorer 7, 8 & 9 are supported. **IE 6 is no longer supported.**

6. The Active KVM Client (AKC), the native Windows Client, requires Internet Explorer 7 or above and Microsoft .NET Framework versions: 3.5, 4.0, 4.0 Client Profile, and 4.0 Extended Profile.

   - Use a URL of the form: http[s]://<KX II address>/akc/.
   - Windows XP, Vista and Windows 7 desktops are supported.

7. **AKC should be used with CC-SG 5.2 when using the Microsoft .NET version 4.0 Framework.** Use CC-SG 5.3. If CC-SG 5.2 must be used, then the user should run AKC standalone once with the specific KX II before using AKC via CC-SG.

8. Firefox releases supported include: Firefox 4 and 6. Sanity testing was done on Firefox 7, 10 and 11. Safari 5.1 is supported. **Firefox version 11 requires JRE version 1.6.0_31, and blocks earlier JRE versions by default.**

9. Firefox versions 4 through 11 have an issue with launching Java Applets using IPv6 addresses. Workaround is to use a hostname or to create a user created security certificate, signed by a Certificate Authority for the KX II and imported it into the Firefox certificate store, marking the certificate as "This certificate can identify websites."

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

11. For iPhone/iPad access, iOS version 4.x is required; we have tested with versions 4.2.1 and 4.3.1.

12. 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 KX II Release 2.2 or upgrade to Mac OS 10.6

    b. **Mac OS 10.5/Power PC**: remain with KX II Release 2.2 or upgrade to Mac OS 10.6

c. **Mac OS 10.5/Intel**: remain with KX II Release 2.2, 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

13. 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.

14. 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.

15. 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.

16. 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.

17. There is a new SNMP v2 MIB. This should be loaded into your SNMP management system if you are enabling SNMP traps from your KX 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 KX 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.

Release 2.5 Important Notes and Information:

1. **New Digital Video CIMs (DVI, HDMI & DisplayPort)**:

a. 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 KX II user interface, defaults to 1280x1024@60hz, but can be changed by the user.

b. 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 KX II documentation for additional suggestions.

c. 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 KX II documentation.

d. Do not change the port’s “Display Native Resolution” during virtual media transfers – it may interrupt the transfer.

e. On Linux, you may need to restart the X window system or reboot the system when changing the “Display Native Resolution.”

f. DVI-D and DVI-I are supported by the D2CIM-DVUSB-DVI, but not DVI-A (less common).

g. 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.

h. The D2CIM-DVUSB-DP does not support DPCP or embedded audio.

2. **Dual Video Support:**

    a. Both the primary and secondary ports should use the same video resolution and port permissions.

    b. The client, the Dominion KX II and the target server should all be configured with the same Primary/Secondary port monitor orientation. Orientation is the spatial relationship of the primary and secondary video displays.

    c. For best results, the Primary Port should be the port with (1) the left-most display (horizontal orientation), or (2) the top display (vertical orientation). Mouse settings, virtual media, Smart Card and digital audio are then controlled from the Primary Port.

    d. Consult the documentation for recommended mouse modes by operating system. The type of extended desktop supported by the video card and/or OS is an important consideration. The mouse mode used for dual video may be different from your single video use.

    e. The use of single mouse mode is not recommended in full screen mode with a single client monitor.

    f. Since two simultaneous KVM sessions are launched, a KX II model supporting 2 or more remote users is required. For multiple servers with dual video ports, an 8 user switch is recommended: DKX2-808 or DKX2-832

3. **SNMPv3:**

    a. Must be enabled on two pages on the user interface:

    b. Device Settings > Event Management – Settings > SNMP Traps Configuration

    c. Device Settings > Device Services > SNMP Agent Configuration

4. **SSL Certificate Vulnerabilities.** Customers running vulnerability scans on the KX II may see violations related to the default SSL certificate installed at the factory. To remove these vulnerabilities, customers should install their own SSL certificate, either self-signed or from a Certificate Authority.

Release 2.4 Important Notes and Information:

1. For the Digital Audio over IP feature:

    a. The D2CIM-DVUSB CIM is required for the audio feature.

    b. The Release 2.4 CIM firmware versions of 3A88 or 5A88 (or greater) is required for the D2CIM-DVUSB. When upgrading to the Release 2.4 firmware, all attached CIMS will be upgraded. For non-attached CIMs, you can use the “CIM Firmware Update” feature to upgrade these CIMS.

    c. Audio performance is dependent on the available network bandwidth. Up to 1.5 mbps is required for CD quality playback (44,100Hz, 16 bits per sample, 2 channels). Round trip network delays exceeding 50 milliseconds or more and packet loss of 1% or greater will result in poor audio quality. In this case, we recommend selecting an audio format that requires less bandwidth. There may be slight breaks in the audio stream based on video processing and other CPU intensive activity.

    d. Since audio utilizes the virtual media connection, when audio is enabled, either a smart card or a mass storage device may be used, but not both. An as an audio session uses bandwidth over the “virtual media” channel, this may affect the performance of virtual media transfers.

    e. When making the audio connection, the USB interface will be re-enumerated, such that a virtual media connection may be interrupted and/or the smart card session may need to be re-authorized.

    f. From a single client workstation, only one simultaneous audio session is supported.

    g. As there is much diversity in Linux’s support of audio, consult the User Guide for more information. Audio is supported for Apple Mac clients, but is not supported on Solaris clients.

    h. For audio recording, ensure that the audio device level is set appropriately on the client PC. Otherwise there may be distortion.

i. Due to varying USB implementations, on some target servers, simultaneous playback and recording may not be supported. Selecting an audio format that requires less bandwidth may be required.

2. In this release, we have expanded the virtual media operations available from Linux and Mac Clients. Please note:

   a. When using the KVM clients on Linux, Linux formatted partitions cannot be mounted on Apple Mac and Windows target servers.

   b. When using the KVM clients on Apple Mac, Mac formatted partitions cannot be mounted on Linux and Windows target servers.

   c. Windows formatted partitions may be mounted on other operating systems.

   d. Active system partitions on Apple Mac and Linux clients should be un-mounted before a virtual media connection.

   e. Linux ext3/4 drive partitions should be un-mounted on the client PC prior to a virtual media connection.

   f. Mapped drives from Mac and Linux clients are not locked and are read-only when mounted on the target server during a virtual media session.

   g. Non-root users on Linux will see the virtual media connection disconnected if a CD ROM is removed from the drive. This is due to the permissions granted to non-root users, and is not the case for root users.

3. Asian language support. For the KVM Clients (VKC, MPC and AKC), set the “Locale Setting of the Client PC” to the appropriate language. For the Remote HTML interface, set the language via the Language item on the Device Settings Menu.

4. When the Auto Scan feature is used to scan tiered target servers, a port change event will be created in the audit log when the server is scanned, and if SNMP notifications are enabled, an SNMP trap will also be generated.

5. For mobile KVM access via Apple iPad and iPhone, CC-SG Release 5.2 or greater is required. Contact the CC-SG Release Notes for more information. For iPhone/iPad access, iOS version 4.x is required; we have tested with versions 4.2.1 and 4.3.1.

6. While Internet Explorer 6 is supported in this release, we recommend using later IE releases due to security concerns. **Internet Explorer 6 is no longer supported as of Release 2.5.**

Release 2.3 (Tiering) Important Notes and Information:

1. For Dominion KXII to KX II tiering:
    a. Two levels of tiering are supported; up to 1024 target servers can be connected. Multiple, tiered KX II switches can be connected to a base KX II switch and accessed either locally or remotely from the base KX II switch.
    b. There are two ways to physically connect the local ports of the tiered switches to the base switch. Use the D2CIM-DVUSB or connect, via Cat5 cable, to the Extended Local Port of the KX2-832 or KX2-864. Since the local port of the tiered switch has been connected to the base switch, local access is not directly available on the tiered switches.
    c. Both local and remote access through the base KX II switch is available. Consolidated local access is a convenient way to access up to 1024 servers from a single console in the data center.
    d. Tiered remote access is also available, but has some restrictions. Non CC-SG customers can connect to the base switch and remotely access all servers connected to the base and tiered switches. Please realize that: (1) there is only one simultaneous tiered connection supported per tiered switch and (2) certain advanced features are not available over a tiered connection. In general, CC-SG or direct access to the tiered switch will provide maximum functionality, although tiered remote access is very convenient for customers needing basic IP access from a single IP address.
    e. Virtual media, smart card and absolute mouse are not available over a tiered connection. These advanced features are available when remotely accessing servers directly from the tiered switches and through CC-SG.
    f. Blade Servers should be connected to the base switch and not to the tiered switches.
    g. CC-SG and MPC provide direct IP access to the base and tiered switches with full support of the advanced features. However, for local access when in the data center, tiering is very useful since up to 1024 servers can be accessed from a single local console.
    h. The base and tiered switches must run the same Dominion KX II Release. Any KX II model can be used as the base and tiered switches. The KX2-832 and KX2-864 are especially recommended as Base Switches. The Dominion KX2-101 and KSX II do not currently support the tiering feature.
    i. Users must share the same login and password on the base and tiered switches.
    j. Note that the boot time for the base switch is dependent on the number of tiered switches connected to it. This is due to synchronization between the base and tiered switches.
    k. For best operation of the tiering feature, we recommend minimizing the number of User Groups, with a maximum of 50 User Groups.
    l. Internet Explorer (IE) 7 is not recommended for tiered remote access. Use IE 8 instead.
2. An additional form of tiering is available in Release 2.4 – generic, hot-key based tiering. In this case a Dominion KX II is the base tier and the tiered switches can be Raritan or 3rd party KVM switches that are hot-key switchable. In this case, the KX II port connected to the KVM switch should be configured to be of type “KVM Switch” on the Port Configuration page. For this form of tiering the following applies:
    a. The D2CIM-VUSB or D2CIM-DVUSB CIM should be used to connect to the local port of the KVM switch to the base switch.
    b. We are not certifying specific KVM switches in Release 2.4.
    c. The tiered KVM switch must support hot-key switching on its local port.
    d. The KVM switch must be configured to accept one of the allowable hot-key sequences and then switch to the selected target server.
    e. Advanced KVM features such as virtual media, smart cards, etc. are not supported over the tiered connection
    f. Consult the KX II documentation for more information.
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):
    a. 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.
    b. You must configure both KX II's for either Private Mode -or- PC-Share Mode
    c. The KX II user group level PC-share permissions are not supported with these CIMs.
    d. Note that CIM name changes are not updated on the other KX II switch until that switch attempts to connect to that port. Port status changes are handled similarly.
    e. You can connect a dual CIM to a KX II and Paragon simultaneously, but then you must configure them both for Private or PC-Share modes.
    f. 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, there were new hardware versions of the D2CIM-VUSB and D2CIM-DVUSB. These CIMs will have a new hardware version: D2CIM-[D]VUSBG2-AA and new firmware versions:
    a. 4Axx for the new D2CIM-VUSB
    b. 5Axx for the new D2CIM-DVUSB

Release 2.2 Important Notes and Information:

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]://<KX 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 KXII 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 KX 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 KX 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 KX 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 KX 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 KX 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:

1. Firefox version 3.0.11 is not supported due to applet loading issues inherent in that release.
2. **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 KX II switch when it is upgraded to Release 2.2. Otherwise upgrade it separately.
3. 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 KX II User Guide.

4. 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 KX II User Guide.

5. 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.

6. 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

7. 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 KX 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

8. The extended local port on the Dominion KX II 8 channel models does not support Smart Card authentication.

9. KX II front-end to Paragon II. Smart Card and Virtual Media are not supported when using Dominion KX II as a front-end to Paragon II. When first accessing the Paragon II OSD through KX II, do not synchronize the mouse manually. A mouse is not needed and may delay the keyboard response for several seconds.

10. The supported distance from KX 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 2.1.8 (DKX2-8xx Models) Important Notes and Information:

1. Please note that the extended local port mirrors the standard local port, extending access to a second location or to a Paragon II switch.

2. With the recommended remote client PC resources, we recommend a maximum of 4 simultaneous KVM sessions on a single remote client workstation.

3. When used with the extended local port, the recommended firmware versions for the UST and EUST User Stations are as follows:

c. P2-UST: V5-1FE - P2 4.5 GA release version or later

d. P2-EUST: EUST-3F0 - P2 4.5 GA release version or later

4. The recommended distance between the extended local port station and the Dominion KX II is given in the table below. The distance can vary according to the type of user station, the video resolution, cable type/quality and environmental conditions.

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

Release 2.1 (Blade Server) Important Notes and Information:

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 KX 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 KX II. Use the appropriate KX 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 KX 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 KX 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 KX 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 and the KSX II products.

11. When blade chassis type ports are connected to the KX II, the User Management Group page must be edited remotely, rather than from the local port.

12. CC-SG 4.1 (or later) is required for use with Release 2.2 and the blade server feature. If you use a previous release of CC-SG, then for blade server chassis with internal KVM switches, you will see the individual blade servers displayed as standard KVM ports, but you will not have blade server functionality. For blade servers directly connected to CIMs, they will be displayed and can be connected to as standard KVM ports, but without the "Port Management" grouping and blade server functionality. Use CC-SG 4.1 for full blade server support.

13. Contact the Dominion KX II documentation, CIM Guide and Blade Configuration Guide or technical support for more information.

Release 2.0.X Important Notes and Information:

1. Both power supplies are monitored by default. If only one power input is plugged in, then the front panel LED will light red. Configure it for a single power input using the "Power Supply Setup" function on the "Device Settings" menu.

2. For reliable network communication, configure the KX II and 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 100Mbps/Full.

3. 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 KX II.

4. 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. **As of Release 2.4, Mac® and Linux clients can now mount these types of media also, subject to the notes above.** Other UNIX based OS' generally do not support virtual media.

5. 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.

6. 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.

7. Please note that the user at the local port can not change the active USB profile. If required, change from one of the remote clients.

8. 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.

9. 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.

10. Be careful of the web browser refresh or reload function/button, which has the side-effect of closing VKC sessions.

11. D2CIM-PWR must be separately ordered. It is not included with the powerstrip.

12. 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.

13. For the best possible video quality, adhere to these distance guidelines from the CIM to the KX II:

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

14. 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.

15. 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” and the “Local Port Settings” are available on the local port. Firmware Update, Backup and Restore, and certain KX II Device Diagnostics features are available from the remote client.

16. 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.

17. External modem usage. 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.

    Recommended modems include: US Robotics (USR) 56K 5686E, Sportster 56K and Courier 56K; and ZOOM v90 & v92. Modem sessions not currently supported from Apple MAC and Linux clients. For best results, when connecting remotely via an external modem to a KX II connected to a USR modem, the remote modem should be the same type of USR modem. Consult the User Guide for more information.

18. 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.

19. 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.

20. An apostrophe (‘) is no longer an allowed character for port (CIM) names.

21. For Mac OS, the Safari™ browser is certified for use in KX Release 2.2. 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.

Firmware Upgrades:

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 KX II in the left navigation panel, or go directly to:

http://www.raritan.com/support/firmwareupgrades/dominionkxii

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.

Please note that the firmware file for the Dominion KX2-808, KX2-832 and KX2-864 models is different from the other Dominion KX II models. There are two firmware files: one for the 1, 2 and 4 user models and a second for the 8 user models. CC-SG can upgrade both firmwares.

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 KX 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 KX II device must be a member of the default Admin Group to have sufficient administrator-level privileges to update the Dominion KX 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 KX 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 KX II using the “Backup / Restore” function on the Maintenance menu on the Remote Console before starting the upgrade..

6. Close any remote or local KX II sessions to all devices connected to the Dominion KX 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 KX 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 KX 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 KX 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 KX 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 KX 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 KX 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 KX II CIMs (D2CIM-VUSB, D2CIM-DVUSB, D2CIM-DVUSB-XXX and D2CIM-PWR) connected to the KX 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 2.1 or later to Release 2.0.

14. In certain tiered configurations, when doing a firmware upgrade on the Base Switch, the user may see a message instructing them to reboot device. If the warning message is seen again, then the user should disable tiering on the device, upgrade the firmware and then re-establish tiering. .

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