



Dominion KX II

User Guide Release 2.0.8

Copyright © 2008 Raritan, Inc.
DKX2-0F-E
January 2008
255-62-4023-00

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior written consent of Raritan, Inc.

© Copyright 2008 Raritan, Inc., CommandCenter®, Dominion®, Paragon® and the Raritan company logo are trademarks or registered trademarks of Raritan, Inc. All rights reserved. Java® is a registered trademark of Sun Microsystems, Inc. Internet Explorer® is a registered trademark of Microsoft Corporation. Netscape® and Netscape Navigator® are registered trademarks of Netscape Communication Corporation. All other trademarks or registered trademarks are the property of their respective holders.

FCC Information

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

VCCI Information (Japan)

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

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



Contents

Chapter 1 Introduction	1
Dominion KX II Overview	2
Virtual Media	3
Product Photos.....	3
Product Features.....	4
Hardware	4
Software	5
Terminology	5
Package Contents	7
User Guide.....	7
Organization of Information.....	8
Related Documentation.....	9
Chapter 2 Getting Started	10
Login Information	10
Default IP Address	10
Supported Operating Systems (Clients) (Shared)	10
Supported Browsers.....	11
Supported Operating Systems and CIMs (Target Servers).....	11
Chapter 3 Installation and Configuration	15
Overview	15
Step 1: Configure KVM Target Servers	16
Supported Video Resolutions.....	16
Desktop Background	17
Mouse Settings.....	17
Operating System Mouse and Video Settings.....	17
Windows XP / Windows 2003 Settings	18
Windows 2000 Settings.....	19
Windows Vista	19
Linux Settings (Red Hat 9)	20
Linux Settings (Red Hat 4)	22
SUSE Linux 10.1 Settings.....	23
Make Linux Settings Permanent	24
Sun Solaris Settings.....	24
IBM AIX 5.3 Settings.....	27

Contents

Make UNIX Settings Permanent	28
Apple Macintosh Settings	28
Step 2 (Optional): Configure Keyboard Language	29
Change the Keyboard Layout Code (Sun Targets)	29
Step 3: Configure Network Firewall Settings	29
Step 4: Connect the Equipment	30
1. AC Power	30
2. Network Ports	31
3. Local Access Port (local PC)	31
4. Target Server Ports	32
Step 5: Dominion KX II Initial Configuration	32
Changing the Default Password	33
Valid Special Characters	33
Assigning an IP Address	35
Naming Target Servers	36
Specifying Power Supply Auto-detection	37
Remote Authentication	37
Note to CC-SG Users	37
Supported Protocols	38
Note on Microsoft Active Directory	38
Authentication vs. Authorization	38
Users, Groups, and Access Permissions	38
Users	39
Groups	39
Relationship between Users and Groups	40

Chapter 4 Connecting to the Dominion KX II 41

User Interfaces	41
Dominion KX II Local Console: Dominion KX II Devices	42
Dominion KX II Remote Console: Dominion KX II Devices	43
Multi-Platform Client (MPC): KX I and Dominion KX II Devices	44
Raritan Remote Client (RRC): Dominion KX II Devices Only	45
Language Support	45
Java Runtime Environment (JRE)	46
Launching the Dominion KX II	46
Dominion KX II Console Layout	48
Dominion KX II Console Navigation	48
Logging Out	49
Dominion KX II Console Menu Tree	49
Managing Favorites	51
Manage Favorites Menu	52
Favorites List	53
Discover Devices - Local Subnet	55
Discover Devices - KX Subnet	57
Add New Favorite	58

Chapter 5 Accessing KVM Target Servers 59

Port Access Page	60
Connecting to a KVM Target Server	61
Port Action Menu	61
Switching Between KVM Target Servers	62
Disconnecting KVM Target Servers	63
Power Controlling a Target Server	63
Power Cycle a Target Server	63
Power On a Target Server	64
Power Off a Target Server	64

Chapter 6 Virtual KVM Client 65

Overview	66
Options	67
Menu Tree	67
Toolbar	68
Mouse Pointer Synchronization	69
Mouse Synchronization Tips	69
Connection Menu	71
Properties Dialog	71
Connection Info	73
Exit	73
Keyboard Menu	74
Send Ctrl+Alt+Delete	74
Keyboard Macros	74
Creating a Keyboard Macro	75
Running a Keyboard Macro	77
Modifying a Keyboard Macro	77
Removing a Keyboard Macro	77
Video Menu	78
Refresh Screen	78
Auto-sense Video Settings	78
Calibrate Color	79
Video Settings	79
Mouse Menu	82
Synchronize Mouse	82
Single Mouse Cursor	83
Standard	83
Intelligent	84
Absolute	84

Contents

Virtual Media	84
Tools Menu.....	85
Options	85
View Menu	86
View Toolbar.....	86
Scaling.....	86
Target Screen Resolution.....	87
Help Menu.....	87
About Raritan Virtual KVM Client.....	87

Chapter 7 Virtual Media 88

Overview	89
Prerequisites for Using Virtual Media.....	91
Using Virtual Media.....	92
Opening a KVM Session.....	93
Connecting to Virtual Media	94
Local Drives	94
Conditions when Read-Write is not Available.....	95
CD-ROM/DVD-ROM/ISO Images	96
Disconnecting Virtual Media	97
File Server Setup (File Server ISO Images Only).....	98

Chapter 8 User Management 100

User Management Menu	100
User List.....	101
Add New User	102
Modify Existing User	103
User Group List	104
Add a New User Group (Shared).....	105
Add New User Group	107
Setting Permissions	109
Setting Port Permissions.....	110
Group-based IP ACL (Access Control List).....	110
Modify Existing User Group	113
Set Permissions for Individual Group.....	114
Change Password	114
Authentication Settings	115
Implementing LDAP Remote Authentication.....	116
Returning User Group Information from Active Directory Server	118
Implementing RADIUS Remote Authentication	120
Returning User Group Information via RADIUS	121
RADIUS Communication Exchange Specifications.....	121

Chapter 9 Device Management 123

Device Management Menu	123
Network Settings	124
Network Basic Settings.....	126
Network Miscellaneous Settings.....	127
LAN Interface Settings	128
Date/Time Settings	130
Event Management	131
Event Management - Settings.....	132
SNMP Configuration	134
Syslog Configuration	136
Event Management - Destinations.....	137
SNMP Agent Configuration	138
SNMP Trap Configuration.....	138
Power Supply Setup Page	141
Port Configuration Page.....	143
Chapter 10 Power Control.....	145
Connect the Power Strip.....	145
Name the Power Strip (Port Page for Power Strips)	147
Associate KVM Target Servers to Outlets (Port Page)	149
Note for D2CIM-VUSB CIM Usage (Shared)	151

Chapter 11 Security Settings 152

Security Settings Menu	152
Security Settings	153
Login Limitations	154
Strong Passwords.....	155
User Blocking.....	156
Encryption & Share.....	157
Checking Your Browser for AES Encryption	160

Contents

IP Access Control.....	160
Chapter 12 Maintenance	163
Maintenance Menu.....	163
Maintenance Features (Local/Remote Console)	163
Audit Log.....	164
Device Information.....	166
Backup and Restore.....	167
CIM Upgrade	169
Upgrade History	171
Reboot	172
Chapter 13 Diagnostics	174
Diagnostics Menu.....	174
Network Interface Page	175
Network Statistics Page	175
Ping Host Page.....	178
Trace Route to Host Page	179
Device Diagnostics	180
Chapter 14 Dominion KX II Local Console	182
Dominion KX II Local Console	183
Physical Connections	184
Reset Button	184
Starting the Dominion KX II Local Console.....	185
Simultaneous Users.....	185
Security and Authentication	186
Dominion KX II Local Console Interface	186
Available Resolutions	186
Accessing KVM Target Servers	187
Server Display.....	187
Hotkeys.....	188
Accessing a Target Server	188
Returning to the Dominion KX II Local Console Interface.....	188
Local Port Administration.....	189
Local Port Settings (Dominion KX II Local Console Only).....	190
Factory Reset (Dominion KX II Local Console Only).....	193
Appendix A Specifications	195
Environmental Requirements.....	195
Physical Specifications.....	195

Computer Interface Modules (CIMs)	197
Remote Connection	198
TCP and UDP Ports Used.....	199
Target Server Connection Distance and Video Resolution.....	200
Network Speed Settings	201
 Appendix B Updating the LDAP Schema	 203
Returning User Group Information	203
From LDAP	203
From Microsoft Active Directory	203
Setting the Registry to Permit Write Operations to the Schema	204
Creating a New Attribute.....	204
Adding Attributes to the Class.....	205
Updating the Schema Cache	207
Editing rcusergroup Attributes for User Members	208
 Appendix C Informational Notes	 212
Overview	212
Non-US Keyboards	213
French Keyboard	213
Caret Symbol (Linux Clients only)	214
Accent Symbol (Windows XP Clients only)	214
Numeric Keypad	215
Tilde Symbol.....	215
Java Runtime Environment (JRE).....	215
Keyboard Language Preference (Fedora Linux Clients).....	216
Macintosh Keyboard	216
Special Sun Key Combinations.....	217
Mouse Pointer Synchronization (Fedora)	217
Resolving Fedora Core Focus	218
SUSE/VESA Video Modes.....	218
CIMs	219
Windows 3-Button Mouse on Linux Targets.....	219
Virtual Media	219
Dell OpTipler and Dimension Computers.....	219
Virtual Media not Refreshed after Files Added	219
Target BIOS Boot Time with Virtual Media	219
CC-SG.....	220
Virtual KVM Client Version not Known from CC-SG Proxy Mode	220
Proxy Mode and MPC	220

Appendix D FAQs	221
General Questions (Shared)	222
Remote Access	224
Universal Virtual Media	226
Ethernet and IP Networking	227
Servers	231
Installation	233
Local Port	235
Power Control	237
Scalability	238
Computer Interface Modules (CIMs)	239
Security	240
Manageability	242
Miscellaneous	243
Troubleshooting	244
Index	245

Chapter 1 Introduction

In This Chapter

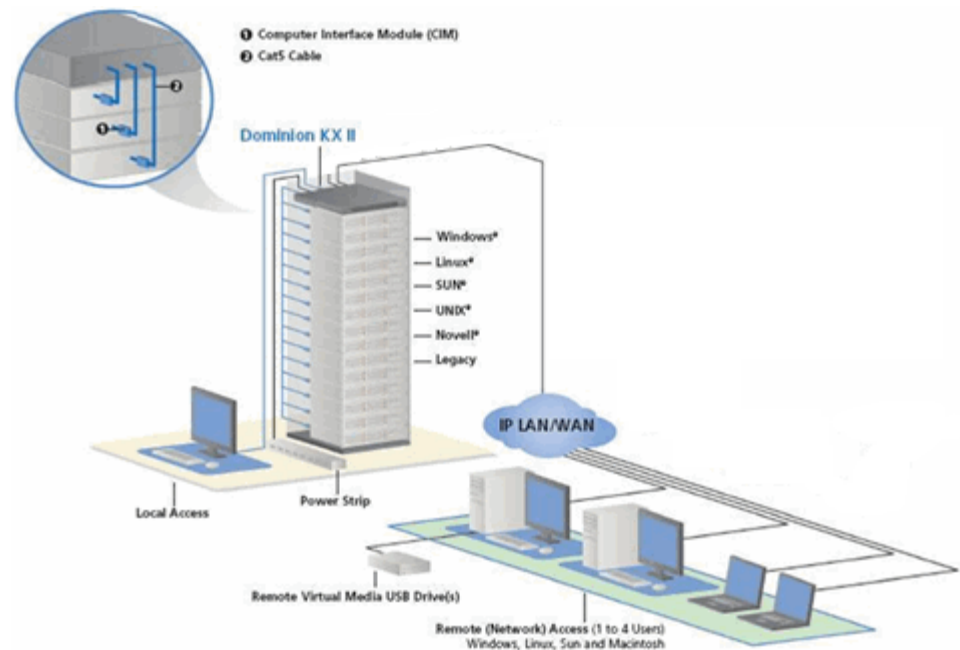
Dominion KX II Overview.....	2
Virtual Media	3
Product Photos	3
Product Features.....	4
Terminology	5
Package Contents.....	7
User Guide.....	7

Dominion KX II Overview

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

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

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



Virtual Media

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

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

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

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

Product Photos



Product Features

Hardware

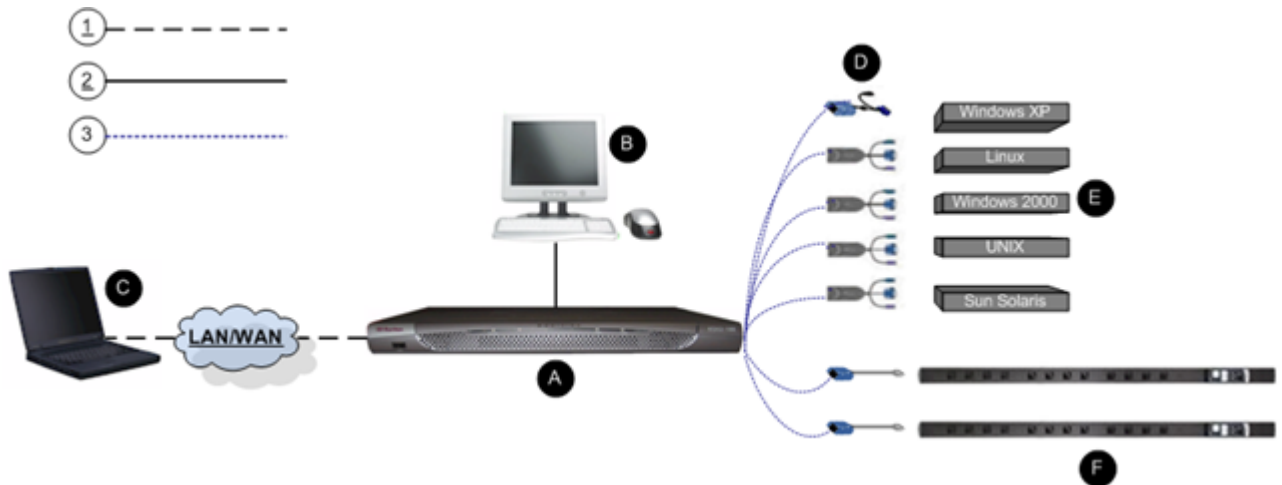
- Integrated KVM-over-IP remote access
- 1U or 2U (KX2-464) rack-mountable; brackets included
- Dual power supplies with failover; auto-switching power supply with power failure warning
- 8, 16, 32, or 64 (on KX2-464) server ports
- Multiple user capacity (1/2/4 remote users; 1 local user)
- UTP (Cat5/5e/6)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

Software

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

Terminology

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



Terminology

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

Package Contents

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

- (1) Dominion KX II Unit
- (1) Dominion KX II Quick Installation and Setup Guide
- (1) Raritan User Manuals CD-ROM
- (1) Rackmount Kit
- (2) AC Power Cords
- (1) Cat5 Network Cable
- (1) Cat5 Network Crossover Cable
- (1) Set of 4 Rubber Feet (for desktop use)
- (1) Application Note
- (1) Warranty Card

User Guide

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

This user guide is specific to Dominion KX II (version 2.0.07); for information pertaining to version 1.4, refer to the Dominion KX 1.4 User Guide.

Organization of Information

The user guide is organized as follows:

- Chapter 1, Introduction. Overview, features, terminology, and package contents
- Chapter 2, Getting Started. Login information; default IP Address; supported operating systems, browsers, and CIMs
- Chapter 3, Installation and Configuration. Target server configuration; firewall settings; physical device connections; initial KX II unit configuration; remote authentication; and users, groups, and access permissions
- Chapter 4, Connecting to the Dominion KX II. User interfaces; starting the KX II Remote Console; Dominion KX II Favorites
- Chapter 5, Accessing Target Servers. Access, control, and switching between target servers
- Chapter 6, Virtual KVM Client. Target server control, mouse pointer synchronization, keyboard macros, and video settings
- Chapter 7, Virtual Media. Virtual media configuration and access
- Chapter 8, User Management. User and group management, passwords, group-based IP access control, and authentication settings
- Chapter 9, Device Management. Network settings, date/time, event management, power supply setup, port configuration, and power control
- Chapter 10, Security Settings. Security settings and IP access control
- Chapter 11, Maintenance. Audit log; device information; backup and restore; firmware and CIM upgrades; and reboot
- Chapter 12, Diagnostics. Network interface, network statistics, ping host, trace route to host, and KX diagnostics
- Chapter 13, KX II Local Console. Starting the KX II Local Console, accessing target servers, and local port administration
- Chapter 14, CC Unmanage. Removing the KX II from CC-SG control
- Appendix A, Specifications. Physical specifications; ports used; target server connection distance and video resolution; and network speed settings
- Appendix B, Updating the LDAP Schema. Update LDAP schema (for experienced users)
- Appendix C, Informational Notes. Important notes on Dominion KX II usage

- Appendix D, FAQs. General questions, remote access, universal virtual media, Ethernet and IP networking, servers, installation, local port, power control, scalability, Computer Interface Modules (CIMs), security, manageability, miscellaneous, and troubleshooting

Related Documentation

For more information about the Raritan Multi-Platform Client (MPC), refer to the Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide.

For more information about the entire Raritan product line, refer to the Raritan User Manuals & Quick Setup Guides CD ROM or Raritan's Web site <http://www.raritan.com/support/productdocumentation>

Chapter 2 Getting Started

In This Chapter

Login Information.....	10
Default IP Address	10
Supported Operating Systems (Clients) (Shared)	10
Supported Browsers	11
Supported Operating Systems and CIMs (Target Servers).....	11

Login Information

- The default Dominion KX II login user name is admin and the default password is raritan. This user has administrative privileges.
- Passwords are case sensitive and must be entered in the exact case combination in which they were created. For example, the default password raritan must be entered entirely in lowercase letters.
- The first time you start the Dominion KX II you are required to change the default password.

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

Default IP Address

Dominion KX II ships with the default IP address of 192.168.0.192.

Supported Operating Systems (Clients) (Shared)

The following operating systems are supported on the Virtual KVM Client™ and Multi-Platform Client (MPC):

Client OS	Virtual Media (VM) Support on Client
Windows XP®	Yes
Windows 2000 SP4®	Yes
Windows Vista®	Yes

Client OS	Virtual Media (VM) Support on Client
Red Hat® Linux 9.0	Yes; Locally held ISO image, Remote File Server mounting directly from Dominion KX II
Red Hat Enterprise Workstation 3.0 and 4.0	Yes; Locally held ISO image, Remote File Server mounting directly from Dominion KX II
SUSE Linux Professional 9.2 and 10	Yes; Locally held ISO image, Remote File Server mounting directly from Dominion KX II
Fedora™ Core 5 and above	Yes; Locally held ISO image, Remote File Server mounting directly from Dominion KX II
Mac®	No
Solaris	No

Supported Browsers

Dominion KX II supports the following browsers:

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

Supported Operating Systems and CIMs (Target Servers)

In addition to the new Dominion KX II D2CIMs, most Paragon® and Dominion KX I CIMs are supported. The following table displays the supported target server operating systems, CIMs, virtual media, and mouse modes:

Note: D2CIM-VUSB is not supported on Sun (Solaris) targets.

Supported Operating Systems and CIMs (Target Servers)

Target Server	Supported CIMs			VM	Mouse Modes		
	Paragon CIMs	Dominion KX I DCIMs	Dominion KX II D2CIMs		AM	IM	SM
Windows XP							
Windows 2000	P2CIM-PS2	DCIM-PS2					
Windows 2000 Server	P2CIM-AUSB	DCIM-USB	D2CIM-VUSB	✓	✓	✓	✓
Windows 2003 Server	UKVMPD	DCIM-USB G2					
Windows Vista	UUSBPD						
Red Hat Linux 9.0	P2CIM-PS2	DCIM-PS2	D2CIM-VUSB				
Red Hat Enterprise Workstation 3.0 and 4.0	P2CIM-AUSB	DCIM-USB	(excluding Red Hat Enterprise Workstation 3.0)	✓			✓
	UKVMPD	DCIM-USB G2					
	UUSBPD						
SUSE Linux Professional 9.2 and 10	P2CIM-PS2	DCIM-PS2	D2CIM-VUSB	✓			✓
	P2CIM-AUSB	DCIM-USB					
	UKVMPD	DCIM-USB G2					
	UUSBPD						
Fedora Core 3 and above	P2CIM-PS2	DCIM-PS2	D2CIM-VUSB	✓			✓
	P2CIM-AUSB	DCIM-USB					
	UKVMPD	DCIM-USB G2					
	UUSBPD						

Target Server	Supported CIMs			VM	Mouse Modes		
	Paragon CIMs	Dominion KX I DCIMs	Dominion KX II D2CIMs		AM	IM	SM
Mac OS	P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓		
All Solaris OSs supported in Dominion KX I	P2CIM-SUN P2CIM-SUSB	DCIM-SUN DCIM-SUSB DCIM-USB G2					✓
IBM AIX	P2CIM-PS2 P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
HP UX	P2CIM-PS2 P2CIM-AUSB UUSBPD	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
Remote Power Strips			D2CIM-PWR				
Serial Devices	P2CIM-SER						

Supported Operating Systems and CIMs (Target Servers)

Legend:

- VM: Virtual Media (D2CIM-VUSB only)
- AM: Absolute Mouse Synchronization (D2CIM-VUSB only)
- IM: Intelligent Mouse Mode
- SM: Standard Mouse Mode
- ✓: Supported

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

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

Chapter 3 Installation and Configuration

In This Chapter

Overview.....	15
Step 1: Configure KVM Target Servers.....	16
Step 2 (Optional): Configure Keyboard Language.....	29
Step 3: Configure Network Firewall Settings	29
Step 4: Connect the Equipment.....	30
Step 5: Dominion KX II Initial Configuration	32
Remote Authentication	37
Users, Groups, and Access Permissions	38

Overview

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

➤ *To install and configure Dominion KX II:*

1. Configure the KVM target servers.
2. (Optional) Configure the keyboard language.
3. Configure the network firewall settings.
4. Connect the equipment.
5. Configure the Dominion KX II unit.

Step 1: Configure KVM Target Servers

KVM target servers are the computers that will be accessed and controlled via the Dominion KX II. Before installing Dominion KX II, configure all KVM target servers to ensure optimum performance. This configuration applies only to KVM target servers, not to the client workstations (remote PCs) used to access Dominion KX II remotely. Refer to *Chapter 1: Introduction, Terminology* (see "Terminology" on page 5) for additional information.

➤ *To configure the KVM target servers:*

- Check the video resolution.
- Check the desktop background.
- Adjust the mouse settings.
- Perform OS-specific mouse and video configuration.

Supported Video Resolutions

Ensure that each target server's video resolution and refresh rate are supported by Dominion KX II and that the signal is non-interlaced.

Video resolution and cable length are important factors in the ability to obtain mouse synchronization. Refer to *Target Server Connection Distance and Video Resolution* (on page 200) for more information. Dominion KX II supports these resolutions:

640x350 @70 Hz	720x400 @85 Hz	1024x768 @90 Hz
640x350 @85 Hz	800x600 @56 Hz	1024x768 @100 Hz
640x400 @56 Hz	800x600 @60 Hz	1152x864 @60 Hz
640x400 @84 Hz	800x600 @70 Hz	1152x864 @70 Hz
640x400 @85 Hz	800x600 @72 Hz	1152x864 @75 Hz
640x480 @60 Hz	800x600 @75 Hz	1152x864 @85 Hz
640x480 @66.6 Hz	800x600 @85 Hz	1152x870 @75.1 Hz
640x480 @72 Hz	800x600 @90 Hz	1152x900 @66 Hz
640x480 @75 Hz	800x600 @100 Hz	1152x900 @76 Hz
640x480 @85 Hz	832x624 @75.1 Hz	1280x960 @60 Hz
640x480 @90 Hz	1024x768 @60 Hz	1280x960 @85 Hz
640x480 @100 Hz	1024x768 @70 Hz	1280x1024 @60 Hz

640x480 @120 Hz	1024x768 @72 Hz	1280x1024 @75 Hz
720x400 @70 Hz	1024x768 @75 Hz	1280x1024 @85 Hz
720x400 @84 Hz	1024x768 @85 Hz	1600x1200 @60 Hz

Note: Composite Sync and Sync-on-Green video require an additional adapter.

Desktop Background

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

Mouse Settings

The Dominion KX II operates in several mouse modes:

- **Absolute Mouse Synchronization** (see "Absolute" on page 84) (D2CIM-VUSB only)
- **Intelligent Mouse Mode** (see "Intelligent" on page 84) (do not use an animated mouse)
- **Standard Mouse Mode** (see "Standard" on page 83)

For both the Standard and Intelligent mouse modes, mouse parameters must be set to specific values, which are described later in this manual. Mouse parameters do not have to be altered for Absolute Mouse Synchronization; D2CIM-VUSB is required for this mode. Mouse configurations will vary on different target operating systems; consult your OS documentation for additional detail.

Intelligent mouse mode generally works well on most Windows platforms. Intelligent mouse mode may produce unpredictable results when active desktop is set on the target. For additional information on Intelligent Mouse mode, refer to the Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide (Appendix B: Conditions for Intelligent Mouse Synchronization) available on Raritan's Website <http://www.raritan.com/support/productdocumentation>, or on the Raritan User Manuals & Quick Setup Guides CD ROM included with your Dominion KX II shipment.

Operating System Mouse and Video Settings

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

Step 1: Configure KVM Target Servers

Windows XP / Windows 2003 Settings

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

1. Configure the mouse settings:
 - a. Choose Start > Control Panel > Mouse.
 - b. Click the Pointer Options tab.
 - c. In the Motion group:
 - Set the mouse motion speed setting exactly to the middle speed.
 - Disable the Enhanced pointer precision option.
 - Click OK.
2. Disable transition effects:
 - a. Select the Display option from Control Panel.
 - b. Click the Appearance tab.
 - c. Click the Effects button.
 - d. Deselect the Use the following transition effect for menus and tooltips option.
 - e. Click OK.
 - f. Close the Control Panel.

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

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

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

Windows 2000 Settings

- *To configure KVM target servers running Microsoft Windows 2000:*
1. Configure the mouse settings:
 - a. Choose Start > Control Panel > Mouse.
 - b. Click the Motion tab.
 - Set the acceleration to None.
 - Set the mouse motion speed setting exactly to the middle speed.
 - Click OK.
 2. Disable transition effects:
 - a. Select the Display option from Control Panel.
 - b. Click the Effects tab.
 - c. Deselect the Use the following transition effect for menus and tooltips option.
 - d. Click OK.
 - e. Close the Control Panel.

Windows Vista

- *To configure KVM target servers running Microsoft Windows Vista:*
1. Configure the mouse settings:
 - a. Choose Start > Settings > Control Panel > Mouse.
 - b. Click the Pointer Options tab.
 - c. In the Motion group:
 - Set the mouse motion speed setting exactly to the middle speed.
 - Disable the Enhanced pointer precision option.
 - Click OK.
 2. Disable animation and fade effects:
 - a. Select the System option from Control Panel.

Step 1: Configure KVM Target Servers

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

Linux Settings (Red Hat 9)

Note: The following settings are optimized for standard mouse mode only.

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

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

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

2. Configure the screen resolution:

- a. Choose Main Menu > System Settings > Display. The Display Settings dialog opens.
- b. From the Display tab, select a Resolution supported by Dominion KX II.
- c. From the Advanced tab, verify that the Refresh Rate is supported by Dominion KX II.

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

- *To configure KVM target servers running Linux (command line):*
1. Set the mouse acceleration to exactly 1 and set the threshold to exactly 1. Enter this command: `xset mouse 1 1`. This should be set for execution upon login.
 2. Ensure that each target server running Linux is using a resolution supported by Dominion KX II at a standard VESA resolution and refresh rate.
 3. Each Linux target server should also be set so the blanking times are within +/- 40% of VESA standard values:
 - a. Go to the Xfree86 Configuration file XF86Config.
 - b. Using a text editor, disable all non-Dominion KX II supported resolutions.
 - c. Disable the virtual desktop feature (not supported by Dominion KX II).
 - d. Check blanking times (+/- 40% of VESA standard).
 - e. Restart computer.

Step 1: Configure KVM Target Servers

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

Note for Red Hat 9 KVM Target Servers

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

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

➤ To configure Red Hat 9 servers using USB CIMs:

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

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

Note: If there is another line using usb-uhci in the /etc/modules.conf file, it needs to be removed or commented out.

3. Save the file.
4. Reboot the system in order for the changes to take effect.

Linux Settings (Red Hat 4)

Note: The following settings are optimized for standard mouse mode only.

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

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

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

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

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

SUSE Linux 10.1 Settings

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

➤ *To configure the mouse settings:*

1. Choose Desktop > Control Center. The Desktop Preferences dialog opens.
2. Click Mouse. The Mouse Preferences dialog opens.
3. Open the Motion tab.
4. Within the Speed group, set the Acceleration slider to the exact center position.
5. Within the Speed group, set the Sensitivity slider to low.
6. Within the Drag & Drop group, set the Threshold slider to small.
7. Click Close.

➤ *To configure the video:*

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

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

Step 1: Configure KVM Target Servers

Make Linux Settings Permanent

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

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

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

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

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

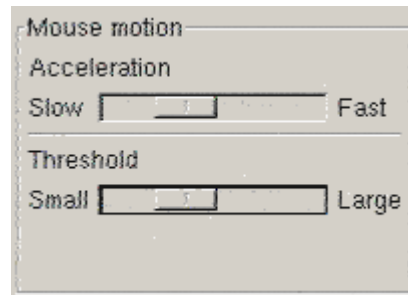
1. Choose Main Menu > Preferences > More Preferences > Sessions. The Session dialog opens.
2. Click the Session Options tab.
3. Deselect the Prompt on the logout checkbox.
4. Select the Automatically save changes to the session checkbox and click **OK**. This option automatically saves your current session when you log out.

Sun Solaris Settings

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

1. Set the mouse acceleration value to exactly 1 and the threshold to exactly 1. This can be performed:

- From the graphical user interface:



- With the command line:

```
xset mouse a t
```

(where “a” is the acceleration and “t” is the threshold.)

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

Display Resolution	Vertical Refresh Rate	Aspect Ratio
1600 x 1200	75 Hz	4:3
1280 x 1024	60,75,85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60,70,75,85 Hz	4:3
800 x 600	56,60,72,75,85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60,72,75,85 Hz	4:3

3. KVM target servers running the Solaris operating system must output VGA video (H-and-V sync, not composite sync).
 - *To change your Sun video card output from composite sync to the non-default VGA output:*
 1. Issue the Stop+A command to drop to bootprom mode.
 2. Issue the following command to change the output resolution:

```
setenv output-device screen:r1024x768x70
```
 3. Issue the “boot” command to reboot the server.

Step 1: Configure KVM Target Servers

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

If you Have:	Use this Video Output Adapter:
Sun 13W3 with composite sync output	APSSUN II Guardian converter
Sun HD15 with composite sync output	1396C converter to convert from HD15 to 13W3 and an APSSUN II Guardian converter to support composite sync
Sun HD15 with separate sync output	APKMSUN Guardian converter

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

Mouse Settings

- *To configure the mouse settings (Sun Solaris 10.1):*
1. Choose Launcher. Application Manager - Desktop Controls opens.
 2. Choose Mouse Style Manager. The Style Manager - Mouse dialog opens.
 3. Set the Acceleration slider to 1.0.
 4. Set the Threshold slider to 1.0.
 5. Click OK.

Accessing the Command Line

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

Video Settings (POST)

Sun systems have two different resolution settings: a POST resolution and a GUI resolution. Please Note that 1024x768x75 is used as an example here; substitute the resolution and refresh rate you are using. Run these commands from the command line.

➤ *To check current POST resolution:*

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

➤ *To change POST resolution:*

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

Video Settings (GUI)

The GUI resolution can be checked and set using different commands depending on the video card in use. Please Note that 1024x768x75 is used as an example here; substitute the resolution and refresh rate you are using. Run these commands from the command line.

The following table is organized by card:

Card	To Check Resolution:	To Change Resolution:
32-bit	<code># /usr/sbin/pgxconfig -prconf</code>	<ol style="list-style-type: none"> 1. <code># /usr/sbin/pgxconfig -res 1024x768x75</code> 2. Logout or restart computer.
64-bit	<code># /usr/sbin/m64config -prconf</code>	<ol style="list-style-type: none"> 1. <code># /usr/sbin/m64config -res 1024x768x75</code> 2. Logout or restart computer.
32-bit and 64-bit	<code># /usr/sbin/fbconfig -prconf</code>	<ol style="list-style-type: none"> 1. <code># /usr/sbin/fbconfig -res 1024x768x75</code> 2. Logout or restart computer.

IBM AIX 5.3 Settings

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

➤ *To configure the mouse:*

1. Go to Launcher.

Step 1: Configure KVM Target Servers

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

➤ *To configure the video:*

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

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

Make UNIX Settings Permanent

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

1. Choose Style Manager > Startup. The Style Manager - Startup dialog opens.
2. Select the Logout Confirmation dialog option of On. This option prompts you to save your current session when you logout.

Apple Macintosh Settings

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

*Note: Enable the Absolute Mouse Scaling for the MAC server option on the **Port** (see "Note for D2CIM-VUSB CIM Usage (Shared)" on page 151) page.*

Step 2 (Optional): Configure Keyboard Language

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

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

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

Change the Keyboard Layout Code (Sun Targets)

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

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

1. Open a Text Editor window on the Sun workstation.
2. Check that the NUM LOCK key is active and press the left CTRL key and the DEL key on your keyboard. The Caps Lock LED starts to blink, indicating that the CIM is in Layout Code Change mode. The text window displays: Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX).
3. Type the layout code desired (for example, 31 for the Japanese keyboard).
4. Press Enter.
5. Shut down the unit and power ON once again. The DCIM-SUSB performs a reset (power cycle).
6. Using MPC, type something to verify that the characters are correct.

Step 3: Configure Network Firewall Settings

To access Dominion KX II through a network firewall, your firewall must allow communication on TCP Port 5000 or another port that you designate. Refer to *Network Settings* (on page 124) for additional information about designating another discovery port.

Step 4: Connect the Equipment

To take advantage of the Dominion KX II:

Web-access capabilities

Automatic redirection of HTTP requests to HTTPS

(i.e., so users can type the more common "http://xxx.xxx.xxx.xxx" instead of "https://xxx.xxx.xxx.xxx")

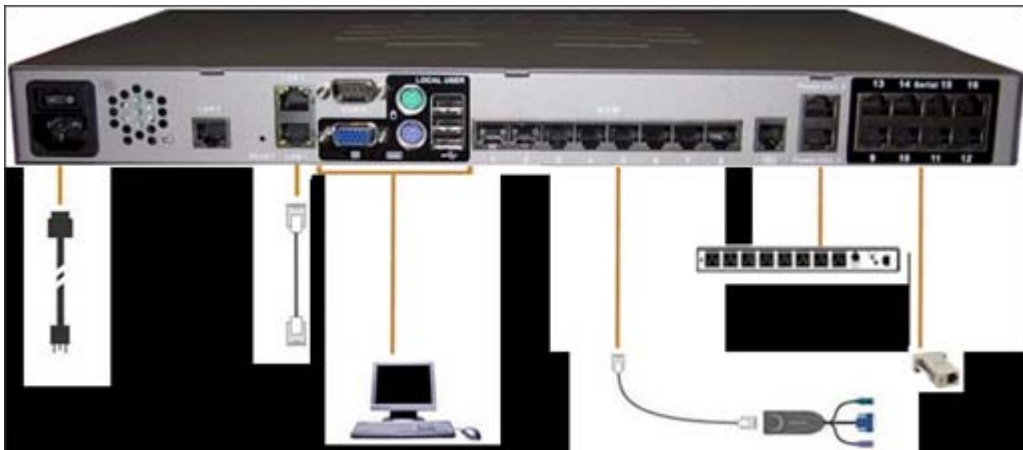
The firewall must allow inbound communication on:

Port 443 - standard TCP port for HTTPS communication

Port 80 - standard TCP port for HTTP communication

Step 4: Connect the Equipment

Connect the Dominion KX II to the power supply, network, local PC, and target servers. The numbers in the diagram correspond to the sections describing the connection.



1. AC Power

➤ *To connect the power supply:*

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

*Note: If you only attach one power cord, the power LED on the Dominion KX II front panel will display red because the system is set to automatically detect both sources. Refer to the **Power Supply Setup Page** (on page 141) for information about turning off automatic detection for the power source not in use.*

2. Network Ports

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

➤ *To connect the network:*

1. Connect a standard Ethernet cable (included) from the network port labeled LAN1 to an Ethernet switch, hub, or router.
2. To make use of the optional Dominion KX II Ethernet failover capabilities:
 - Connect a standard Ethernet cable from the network port labeled LAN2 to an Ethernet switch, hub, or router.
 - Enable Automatic Failover on the Network Configuration screen (refer to **Network Settings, LAN Interface Settings** (see "LAN Interface Settings" on page 128) for more information).

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

3. Local Access Port (local PC)

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

➤ *To connect the local port:*

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

Step 5: Dominion KX II Initial Configuration

4. Target Server Ports

Dominion KX II uses standard UTP cabling (Cat5/5e/6) to connect to each target server. Refer to *Appendix A: Specifications* (see "Specifications" on page 195) for additional information.

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

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

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

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

Step 5: Dominion KX II Initial Configuration

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

- Change the default password.
- Assign the IP Address.
- Name the KVM target servers and serial targets.

Changing the Default Password

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

➤ *To change the default password:*

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

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

Note: The default password can also be changed from the Raritan Multi-Platform Client (MPC). For more information, refer to the Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide.

Valid Special Characters

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

Step 5: Dominion KX II Initial Configuration

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

Assigning an IP Address

These procedures describe how to assign an IP Address using the Network Settings page. For complete information about all of the fields and the operation of this page, refer to *Network Settings* (on page 124).

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

Port Access | Virtual Media | User Management | **Device Settings** | Security | Maintenance | Diagnostics

Home > Device Settings > Network Settings

Network Basic Settings

Device Name *

IP auto configuration

Preferred host name (DHCP only)

IP address

Subnet mask

Gateway IP address

Primary DNS server IP address

Secondary DNS server IP address

Network Miscellaneous Settings

Discovery Port *

Bandwidth Limit

LAN Interface Settings

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

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

LAN Interface Speed & Duplex

☐ Enable Automatic Fallover

Ping Interval (seconds) *

Timeout (seconds) *

2. Specify a meaningful Device Name for your Dominion KX II unit; up to 16 alphanumeric characters, *special characters* (see "Valid Special Characters" on page 33), and no spaces.
3. Choose the IP auto configuration from the drop-down list:
 - None (Static IP). This option requires that you manually specify the network parameters. This is the recommended option because the Dominion KX II is an infrastructure device and its IP Address should not change.
 - DHCP. With this option, network parameters are assigned by the DHCP server.

Step 5: Dominion KX II Initial Configuration

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

Your Dominion KX II unit is now network accessible.

*Note: In some environments, the LAN Interface Speed & Duplex setting default of Autodetect (auto-negotiation) does not properly set the network parameters, resulting in network issues. In these instances, setting the Dominion KX II LAN Interface Speed & Duplex field to 100 Mbps/Full Duplex (or whatever option is appropriate to your network) addresses the issue. Refer to the **Network Settings** (on page 124) page for more information.*

Naming Target Servers

➤ *To name the target servers:*

1. Connect all of the target servers if you have not already done so (as described in **Step 3: Connect the Equipment, Target Server Ports** (see "4. Target Server Ports" on page 32)).
2. Using the Dominion KX II Local Console, choose Device Settings > Port Configuration. The Port Configuration page opens:

Port Configuration

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

3. Click on the Port Name of the target server you want to rename. The **Port Page** (see "Associate KVM Target Servers to Outlets (Port Page)" on page 149) opens.
4. Assign a name to identify the server connected to that port. The name can be up to 32 characters; alphanumeric and *special characters* (see "Valid Special Characters" on page 33) are allowed.
5. Click OK.

Specifying Power Supply Auto-detection

The Dominion KX II provides dual power supplies, and can automatically detect and provide notification regarding the status of these power supplies. Proper configuration ensures that the Dominion KX II sends the appropriate notifications should a power supply fail. The Power Supply Setup page is configured to automatically detect both power supplies; use this page to disable automatic detection of the power supply not in use.

➤ *To disable power supply auto-detection for the power supply not in use:*

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

For more information, refer to **Power Supply Setup Page** (on page 141).

Remote Authentication

Note to CC-SG Users

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

For additional information about CC-SG authentication, refer to the CommandCenter Secure Gateway User Guide, Administrator Guide, or Deployment Guide at:

<http://www.raritan.com/support/productdocumentation>.

Supported Protocols

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

Note on Microsoft Active Directory

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

Authentication vs. Authorization

Authentication is the process of verifying that a user is who he says he is. Once a user is authenticated, the user's group is used to determine his system and port permissions. The user's assigned privileges determine what type of access is allowed. This is called authorization.

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

Users, Groups, and Access Permissions

The Dominion KX II stores an internal list of all user and group names to determine access authorization and permissions. This information is stored internally in an encrypted format. There are several forms of authentication and this one is known as "local authentication". All users have to be authenticated; if Dominion KX II is configured for LDAP/LDAPS or RADIUS, that authentication is processed first, followed by local authentication.

Users

The Dominion KX II stores an internal list of all user and group names to determine access authorization and permissions. This information is stored internally in an encrypted format. There are several forms of authentication and this one is known as “local authentication”. All users have to be authenticated; if Dominion KX II is configured for LDAP/LDAPS or RADIUS, that authentication is processed first, followed by local authentication.

User names and passwords are required to gain access to the Dominion KX II unit. This information is used to authenticate users attempting to access your Dominion KX II unit. Refer to User Management for more information about adding and editing users.

Groups

Every Dominion KX II unit is delivered with three default user groups; these groups cannot be deleted:

Admin	Users that are a member of this group have full administrative privileges. The original, factory-default user is a member of this group and has the complete set of system privileges. In addition, the Admin user must be a member of the Admin group.
Unknown	This is the default group for users who are authenticated externally using LDAP/LDAPS or RADIUS or who are unknown to the system. If the external LDAP/LDAPS or RADIUS server does not identify a valid user group, the Unknown group is used. In addition, any newly created user is automatically put in this group until assigned to another group.
Individual Group	An individual group is essentially a “group” of one. That is, the specific user is in its own group, not affiliated with other real groups. Individual groups can be identified by the “@” in the Group Name. The individual group allows a user account to have the same rights as a group.

In addition to the system-supplied default groups, you can create groups and specify the appropriate permissions to suit your needs. Refer to User Management for more information about creating and editing user groups.

Relationship between Users and Groups

Users belong to a group and groups have privileges. Organizing the various users of your Dominion KX II into groups saves time by allowing you to manage permissions for all users in a group at once, instead of managing permissions on a user-by-user basis.

You may also choose not to associate specific users with groups. In this case, you can classify the user as “Individual.”

Upon successful authentication, the device uses Group information to determine the user's permissions - which server ports are accessible, whether rebooting the unit is allowed, and other features.

Chapter 4 Connecting to the Dominion KX II

In This Chapter

User Interfaces.....	41
Dominion KX II Local Console: Dominion KX II Devices.....	42
Dominion KX II Remote Console: Dominion KX II Devices.....	43
Multi-Platform Client (MPC): KX I and Dominion KX II Devices	44
Raritan Remote Client (RRC): Dominion KX II Devices Only	45
Language Support	45
Java Runtime Environment (JRE)	46
Launching the Dominion KX II.....	46
Managing Favorites.....	51

User Interfaces

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

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

Dominion KX II Local Console: Dominion KX II Devices

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

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

- **Local Port Settings** (see "Local Port Settings (Dominion KX II Local Console Only)" on page 190)
- **Factory Reset** (see "Factory Reset (Dominion KX II Local Console Only)" on page 193)

Dominion KX II Remote Console: Dominion KX II Devices

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

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

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

- *Virtual Media* (on page 88)
- *Favorites* (see "Managing Favorites" on page 51)
- *Backup/Restore* (see "Backup and Restore" on page 167)
- Firmware Upgrade
- *Upgrade Report* (see "Upgrade History" on page 171)
- *Diagnostics* (see "Device Diagnostics" on page 180)

Multi-Platform Client (MPC): KX I and Dominion KX II Devices

The Raritan Multi-Platform Client (MPC) is a graphical interface that allows you to remotely access the target devices connected to Dominion units. MPC can be installed for standalone use or accessed through a Web browser.

After installing the Dominion KX II, either download a standalone version of Raritan MPC and establish an initial network connection, or launch the application directly.

Note: MPC supports both KX I and Dominion KX II devices; use MPC if you would like to access servers connected to both KX I and Dominion KX II devices with one user interface.

➤ *To launch MPC directly:*

1. To launch MPC from a client running any browser, type `http://IP-ADDRESS/mpc` into the address line, where IP-ADDRESS is the IP address of your Raritan device. MPC will launch in a new window that does not contain a menu bar, tool bar, scroll bar, or address bar. Work in this window and toggle to other open windows using the ALT+TAB command.
2. When MPC launches, a device tree of all automatically detected Raritan devices found on your subnet is displayed on the left side of the screen. If you do not find your Dominion KX II unit listed by name, create an icon manually by choosing **Connection > New Profile**. The Add Connection window opens.
3. Type a device Description, specify a Connection Type, add the Dominion unit's IP Address, and click OK. These specifications can be edited later.
4. In the Navigator panel on the left of the screen, double-click on the icon that corresponds to your Dominion KX II unit.

Refer to the Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide, available on Raritan's Website <http://www.raritan.com/support/productdocumentation>, or on the Raritan User Manuals & Quick Setup Guides CD ROM included with your Dominion shipment for complete information on installing and operating MPC.

Raritan Remote Client (RRC): Dominion KX II Devices Only

Raritan Remote Client (RRC) is a graphical user interface providing remote access to the target devices.

Note: RRC cannot be used with the Dominion KX II; use MPC instead.

Language Support

The Dominion KX II provides keyboard support for the following languages: US English, UK English, Traditional Chinese, Simplified Chinese, Japanese, Korean, French, German, Belgian, Norwegian, Danish, and Swedish.

Note: You can use the keyboard for Chinese, Japanese, and Korean for display only; local language input is not supported at this time for Dominion KX II Local Console functions.

For more information about non-US keyboards, see **Appendix C: Informational Notes** (see "Informational Notes" on page 212).

Language	Regions	Keyboard Layout
US English	United States of America and most of English-speaking countries: e.g. Canada, Australia, and New Zealand.	US Keyboard layout.
US English International	United States of America and most of English-speaking countries: e.g. Netherlands	US Keyboard layout.
UK English	United Kingdom	UK layout keyboard
Chinese Traditional	Hong Kong S. A. R., Republic of China (Taiwan)	Chinese Traditional
Chinese Simplified	Mainland of the People's Republic of China	Chinese Simplified
Korean	South Korea	Dubeolsik Hangul
Japanese	Japan	JIS Keyboard
French	France	French (AZERTY) layout keyboard.

Java Runtime Environment (JRE)

Language	Regions	Keyboard Layout
German	Germany and Austria	German keyboard (QWERTZ layout).
Belgium	Belgium	Belgian
Norway	Norway	Norwegian
Denmark	Denmark	Danish
Sweden	Sweden	Swedish

Java Runtime Environment (JRE)

Important: It is recommended that you disable Java caching and clear the Java cache. Please refer to your Java documentation or the Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide for more information.

The Dominion KX II Remote Console and MPC require the JRE to function. The Dominion KX II Remote Console checks the Java version; if the version is incorrect or outdated, you will be prompted to download a compatible version.

Raritan recommends using Java Runtime Environment (JRE) version 1.5 for optimum performance, but the Dominion KX II Remote Console and MPC will function with JRE version 1.4.2_05 or greater (with the exception of JRE 1.5.0_02), including JRE 1.6.

Note: In order for multi-language keyboards to work in the Dominion KX II Remote Console (Virtual KVM Client) please install the multi-language version of Java Runtime Environment (JRE).

Launching the Dominion KX II

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

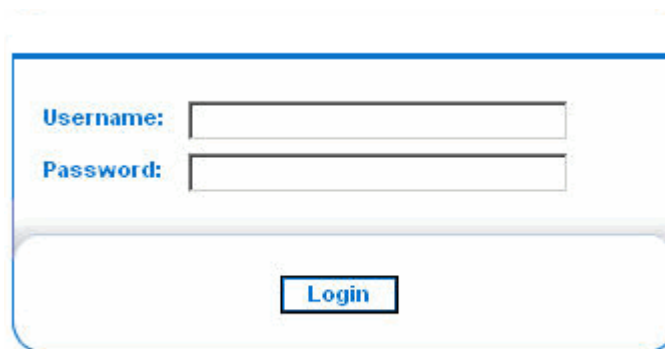
Depending on your browser and security settings, you may see various security and certificate warnings. It is necessary to accept these warnings to launch the Dominion KX II Remote Console.

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

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

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

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



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

Launching the Dominion KX II

Dominion KX II Console Layout

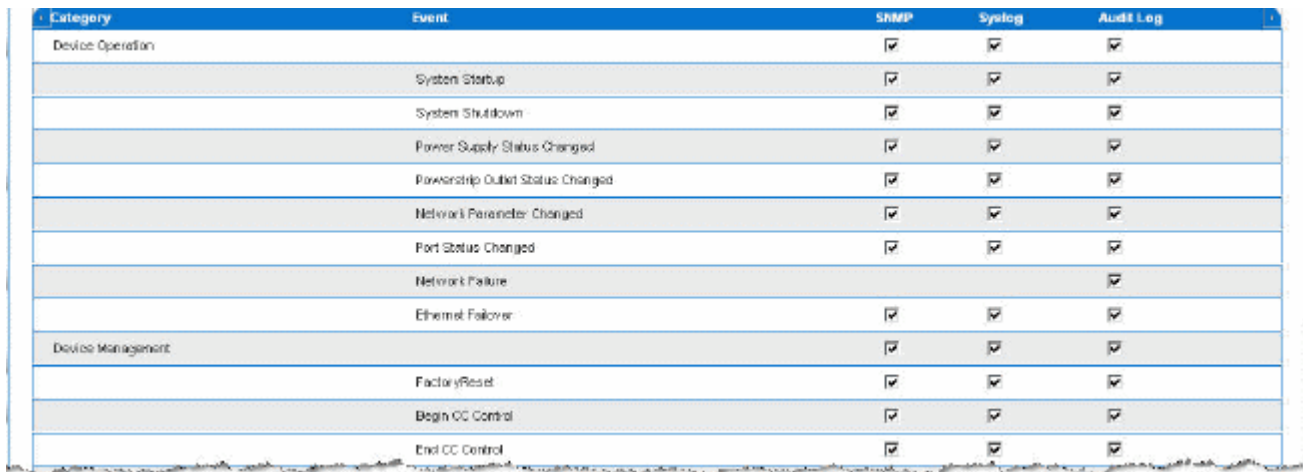
Both the Dominion KX II Remote Console and the Dominion KX II Local Console interfaces provide an HTML (web-based) interface for configuration and administration, as well as target server list and selection. The options are organized into various tabs.

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

Dominion KX II Console Navigation

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

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



Category	Event	SNMP	Syslog	Audit Log
Device Operation		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Startup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Power Supply Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Powerstrip Outlet Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Parameter Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Failure			<input checked="" type="checkbox"/>
	Ethernet Failover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Management		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	FactoryReset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Begin OC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	End OC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- *To scroll through pages longer than the screen:*
- Use Page Up and Page Down keys on your keyboard, or
 - Use the scroll bar on the right

For more information about navigation and selection in the Raritan Multi-Platform Client (MPC), refer to the Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide.

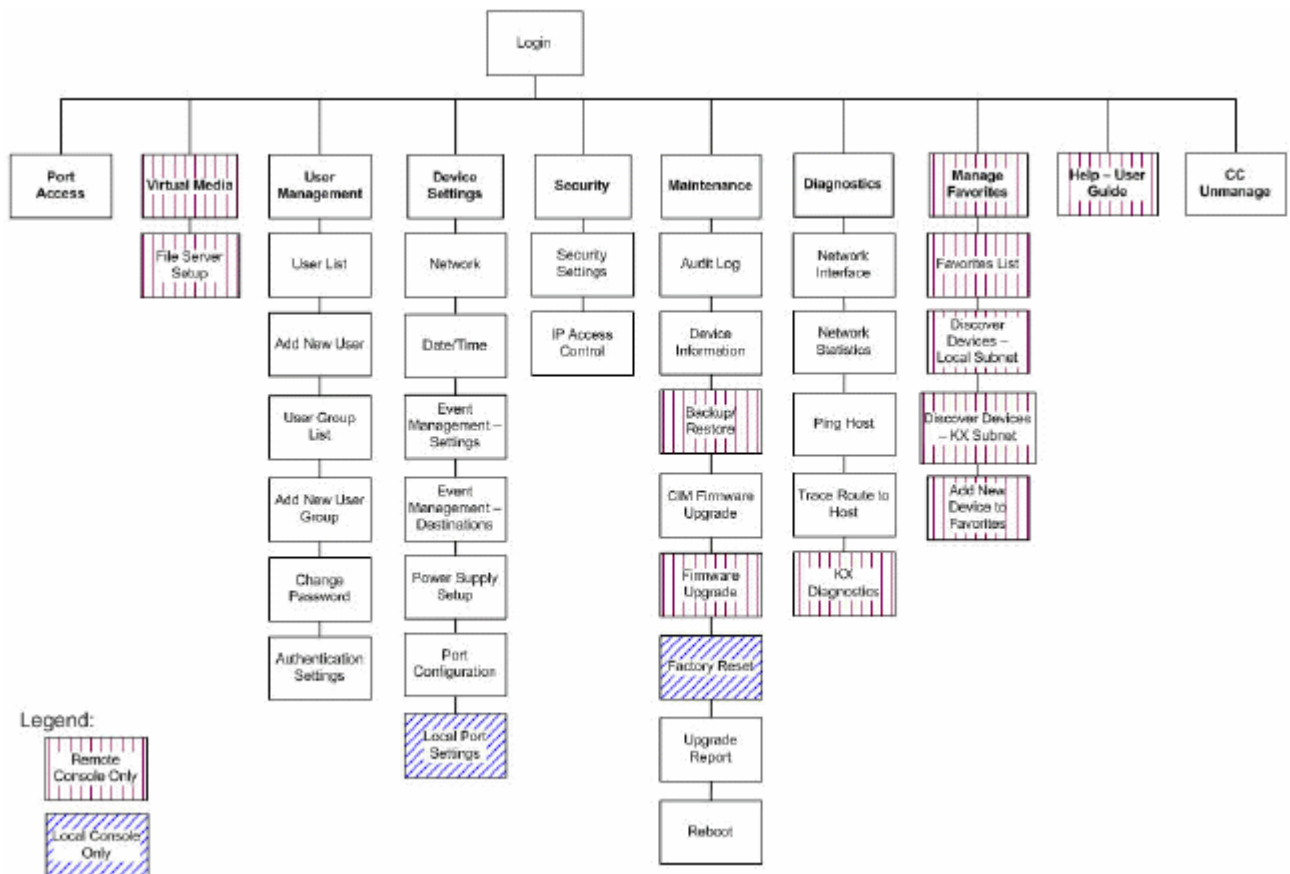
Logging Out

- *To quit the Dominion KX II Remote Console:*
- Click Logout in the upper right-hand corner of the page.

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

Domainion KX II Console Menu Tree

The following diagram represents all of the menu options available in both the Dominion KX II Remote and Dominion KX II Local Console interfaces. Variations between the Dominion KX II Local Console and the Dominion KX II Remote Console are identified.



Launching the Dominion KX II

In addition to being identified in the menu tree above, menu option variations between the Dominion KX II Local Console and the Dominion KX II Remote Console are identified in the following table:

Option	Local Console	Remote Console
Virtual Media		✓
File Server Setup		✓
Backup/Restore		✓
Firmware Upgrade		✓
KX Diagnostics		✓
Manage Favorites		✓
Favorites List		✓
Discover Devices - Local Subnet		✓
Discover Devices - KX Subnet		✓
Add New Device to Favorites		✓
Help - User Guide		✓
Local Port Settings	✓	
Factory Reset	✓	

Managing Favorites

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

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

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

Port Access

Click on the individual port name to see allowable operations.
0 of 1 Remote KVM channels currently in use.

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

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

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

Managing Favorites

- *To toggle the Favorite Devices list display between name and IP Address:*

To display Favorites by IP Address:

Click the Display by IP button.

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



To display Favorites by name:

Click the Display by Name button.

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



Manage Favorites Menu

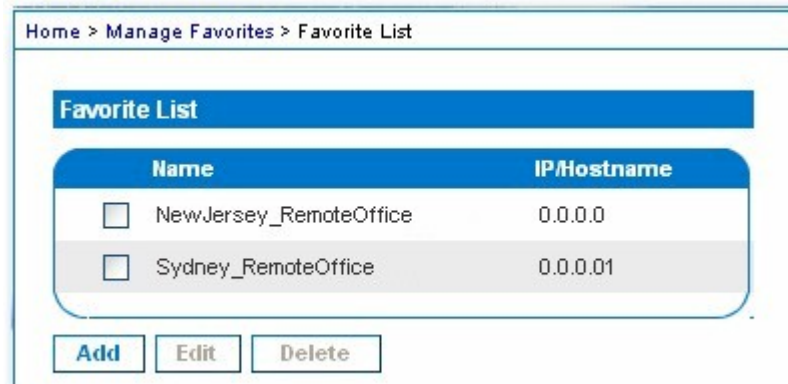
- *To open the Manage Favorites menu:*
- Click the Manage button. The Manage Favorites page opens and contains the following:

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

Favorites List

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

- *To open the Favorites List page:*
 - Choose Manage > Favorites List. The Favorites List page opens:



- *To add a Favorite:*
 - Click the Add button. The *Add New Favorite* (on page 58) page opens.
- *To delete a Favorite:*

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

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

- *To edit a Favorite:*
 1. From the Favorites List page, select the checkbox next to the appropriate Dominion KX II device.
 2. Click the Edit button. The Edit page opens:

Managing Favorites

Home > Manage Favorites > Edit / Delete Favorites > Editing: 0.0.0.0

Edit: 0.0.0.0

All fields are required

Description

IP Address

Port

Home > Manage Favorites > Favorite List > Add New Favorite

Add New Favorite

All fields are required

Description

IP Address

Port

Product Type

▼

3. Update the fields as necessary:
 - Description. Type something meaningful.
 - IP Address. Type the IP Address of the Dominion KX II unit.
 - Port. Change the discovery Port (if necessary).
 - Product Type
4. Click OK.

Discover Devices - Local Subnet

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

Port Access Virtual Media User Management Device Settings Security Main

Home > Manage Favorites > Discover Devices - Local Subnet

Discover Devices - Local Subnet

☒ Use Default Port 5000

Discover on Port:

5000

Save

Name	IP/Hostname
<input type="checkbox"/> Annettes_KX116	192.168.59.213
<input type="checkbox"/> Annettes_KX432	192.168.59.227
<input type="checkbox"/> ASTDKXII-416	192.168.59.218
<input type="checkbox"/> buntkox	192.168.59.217
<input type="checkbox"/> DaveKX2	192.168.59.206
<input type="checkbox"/> Dominion-KX	192.168.59.240
<input type="checkbox"/> DominionKX	192.168.59.224
<input type="checkbox"/> DominionKX	192.168.59.225
<input type="checkbox"/> DominionKX	192.168.59.237
<input type="checkbox"/> DominionKX	192.168.59.239
<input type="checkbox"/> DominionKX	192.168.59.244
<input type="checkbox"/> DominionKX	192.168.59.249
<input type="checkbox"/> DominionKX	192.168.59.252
<input type="checkbox"/> DominionKX	192.168.59.253
<input type="checkbox"/> kox14	192.168.59.233
<input type="checkbox"/> kox2wrc4	192.168.59.185
<input type="checkbox"/> IrakKX2	192.168.59.207
<input type="checkbox"/> shivas_kox20	192.168.59.208

Select All Deselect All

Add Refresh

Copyright © 2007 Raritan Computer Inc.

Managing Favorites

➤ *To discover devices on the local subnet:*

1. Choose Favorites > Discover Devices - Local Subnet. The Discover Devices - Local Subnet page opens.
2. Choose the appropriate discovery port (refer to *Network Miscellaneous Settings* (on page 127) for information about the discovery port):
 - To use the default discovery port, select the Use Default Port 5000 option.
 - To use a different discovery port:
 - a. Deselect the Use Default Port 5000 option.
 - b. Type the port number into the Discover on Port field.
 - c. Click Save.
3. Click Refresh. The list of devices on the local subnet is refreshed.

➤ *To add devices to your Favorites List:*

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

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

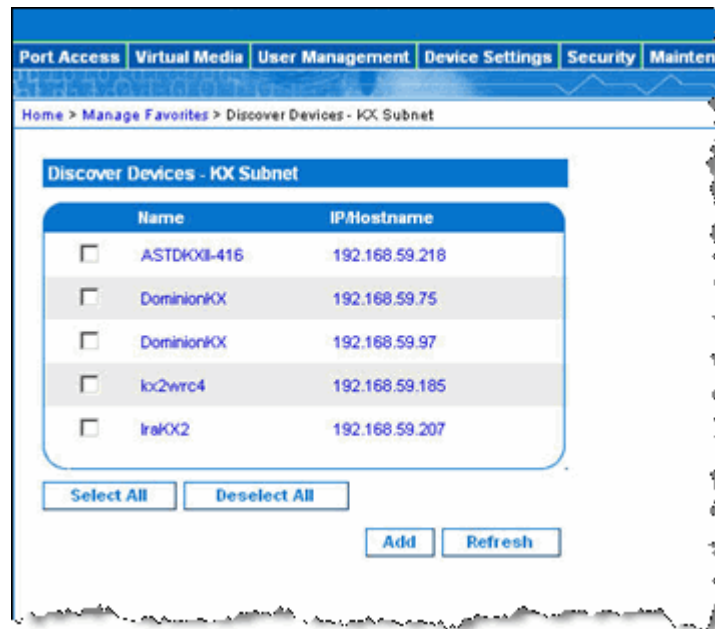
➤ *To access a discovered device:*

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

Discover Devices - KX Subnet

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

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



➤ *To discover devices on the device subnet:*

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

➤ *To add devices to your Favorites List:*

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

Managing Favorites

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

➤ *To access a discovered device:*

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

Add New Favorite

➤ *To add a device to your favorites list:*

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

This device is added to your list of favorites.

Chapter 5 Accessing KVM Target Servers

You are able to connect to KVM and Serial devices using the following:

- Multi-Platform Client (MPC)
- Standalone Raritan Remote Client (RRC)
- Via the Port Access Page

In This Chapter

Port Access Page	60
Connecting to a KVM Target Server	61
Port Action Menu	61
Switching Between KVM Target Servers	62
Disconnecting KVM Target Servers	63
Power Controlling a Target Server.....	63

Port Access Page

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

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

➤ To use the Port Access page:

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

Port Access

Click on the individual port name to see allowable operations.
0 of 1 Remote KVM channels currently in use.

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

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

- Port Number. Numbered from 1 to the total number of ports available for the Dominion KX II unit. Please note that ports connected to power strips will not be among those listed, resulting in gaps in the Port Number sequence.

- **Port Name.** The name of the Dominion KX II port; initially set to Dominion-KX2-Port#, but you can change the name to something more descriptive. When you click on a Port Name link, the Port Action Menu is opened.
 - **Status.** The status is either up or down.
 - **Availability.** The Availability can be Idle, Connected, Busy, or Unavailable.
2. Click the Port Name of the target server you want to access. The Port Action Menu is displayed. Refer to ***Port Action Menu*** (on page 61) for more information about the menu options available.
 3. Choose the desired menu option from the Port Action Menu.
- *To change the display sort order:*
- Click the column heading you want to sort on. The list of KVM target servers is sorted by that column.

Connecting to a KVM Target Server

- *To connect to a KVM target server:*
1. From the Dominion KX II Remote Console, click the Port Access tab to open it. The Port Access page opens.
 2. Click the Port Name of the target you want to access. The Port Action menu is displayed.
 3. Click Connect. A ***Virtual KVM Client*** (on page 65) window opens to the target server connected to that port.

Port Action Menu

1. When you click on a Port Name in the Port Access list, the **Port Action** menu is displayed. Please note that only options available for the selected port are listed in the **Port Action** menu:
 - **Connect.** Creates a new connection to the target server. For the Dominion KX II Remote Console, a new ***Virtual KVM Client*** (on page 65) window is opened. For the Dominion KX II Local Console, the display switches to the target server and switches away from the local user interface. On the local port, the Dominion KX II Local Console interface must be visible in order to perform the switch.

Switching Between KVM Target Servers

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

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

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

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

Note: This menu item is not available on the Dominion KX II Local Console; the only way to disconnect from the switched target in the Local Console is to use the *hotkey* (see "Hotkeys" on page 188).

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

2. Choose the desired menu option for that port to execute it.

Switching Between KVM Target Servers

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

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

➤ *To switch between KVM target servers:*

1. While already using a target server, access the Dominion KX II Port Access page.

2. Click the Port Name of the target you want to access now. The Port Action menu is displayed.
3. Choose the Switch From option from the Port Action menu. The *Virtual KVM Client* (on page 65) window switches to the new target server you selected.

Disconnecting KVM Target Servers

*Note: This item is not available on the Dominion KX II Local Console; the only way to disconnect from the switched target in the Local Console is to use the **hotkey** (see "Hotkeys" on page 188).*

➤ *To disconnect a target server:*

1. Click the Port Name of the target you want to disconnect. The Port Action menu is displayed.
2. Choose the Disconnect option from the Port Action menu.

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

Power Controlling a Target Server

Note: These features are available only when you have made power associations. Refer to power control for more information.

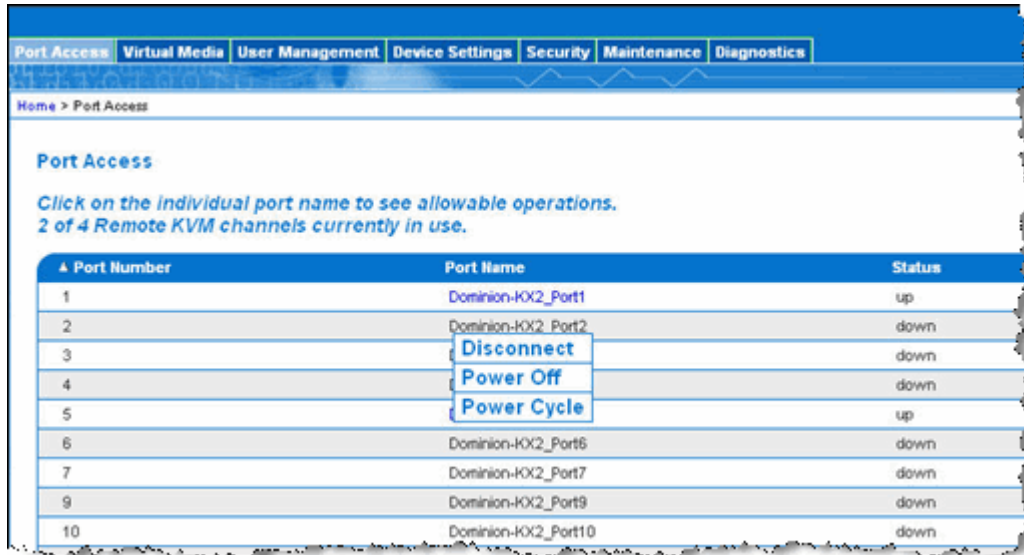
Power Cycle a Target Server

➤ *To power cycle a KVM target server:*

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

Power Controlling a Target Server

- Click the Port Name of the appropriate target server. The Port Action menu is displayed.



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

Power On a Target Server

➤ *To power ON a target server:*

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

Power Off a Target Server

➤ *To power OFF a target server:*

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

Chapter 6 Virtual KVM Client

In This Chapter

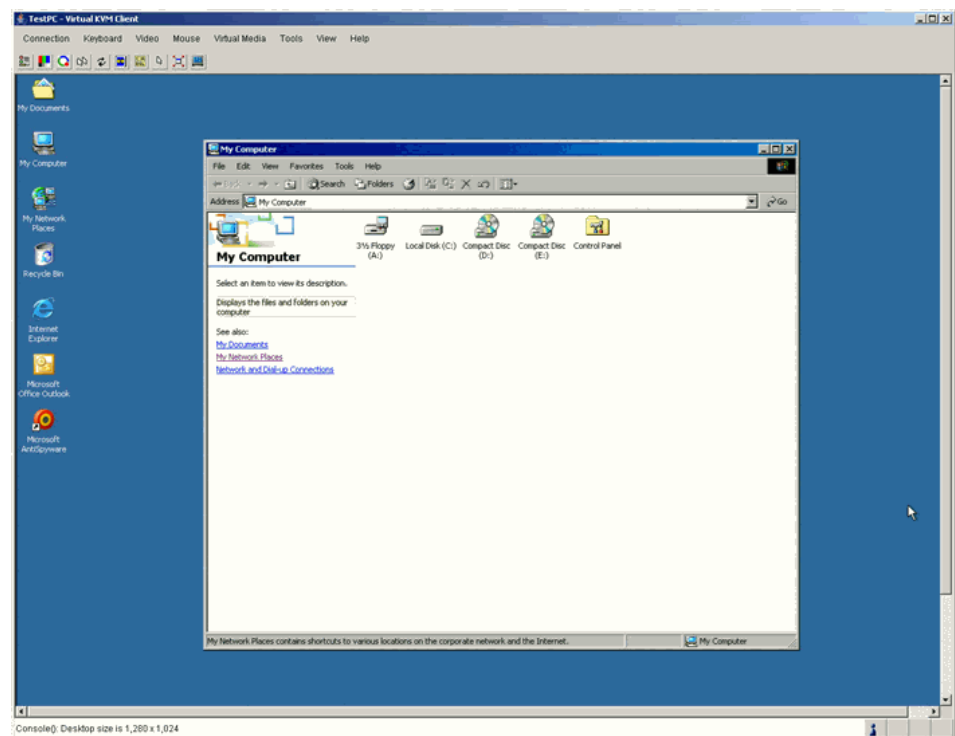
Overview.....	66
Options.....	67
Mouse Pointer Synchronization.....	69
Connection Menu	71
Keyboard Menu	74
Video Menu	78
Mouse Menu.....	82
Virtual Media	84
Tools Menu	85
View Menu	86
Help Menu.....	87

Overview

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

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

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



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

Feature	Description
Menu Bar	Drop-down menus of commands and settings.
Toolbar	Shortcut buttons to frequently used features and commands.

Feature	Description
Target Server Video Window	Target device display.
Status Bar	Real-time information on connection parameters, target server window size, concurrent connections, Caps Lock indicator, and Num Lock indicator.

Options

Menu Tree











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

- Connection
 - Properties
 - Connection Info
 - Exit
- Keyboard
 - Send Ctrl + Alt + Delete
 - Keyboard Macros
 - User-Created Macros (Optional)
- Video
 - Refresh Screen
 - Auto-Sense Video Settings
 - Calibrate Color
 - Video Settings
- Mouse
 - Synchronize Mouse
 - Single Mouse Cursor
 - Absolute
 - Intelligent
 - Standard

Options

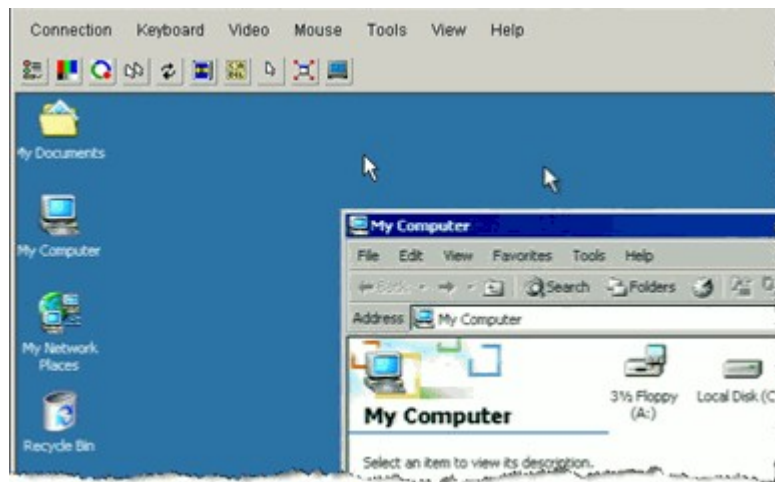
- Virtual Media
 - Connect Drive
 - Connect CD-ROM/ISO Image
- Tools
 - Options
- View
 - View Toolbar
 - Scaling
 - Target Screen Resolution
- Help
 - About Raritan Virtual KVM Client

Toolbar

Button	Description
	Properties
	Video settings
	Calibrate color
	Synchronize client and target server mouse cursors
	Refresh screen
	Auto-sense video
	Send Ctrl+Alt+Delete
	Toggles single/double mouse modes
	Full screen
	Resize video to fit screen

Mouse Pointer Synchronization

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




On fast LAN connections, you may want to disable the Virtual KVM Client mouse pointer and view only the target server's pointer. You can toggle between these two modes (single mouse and dual mouse). Refer to *Mouse Menu* (on page 82) for additional information about the available mouse modes.

Mouse Synchronization Tips

Be sure to follow these steps when obtaining mouse synchronization:

1. Verify that the selected video resolution and refresh rate is among those supported by the Dominion KX II. The Virtual KVM Client Connection Info dialog displays the actual values that the Dominion KX II is seeing. Please refer to Supported Video Resolutions for more information about the video resolutions that are supported.
2. Verify that the cable length is within the specified limits for the selected video resolution. Please refer to *Target Server Connection Distance and Video Resolution* (on page 200) for more information.

Mouse Pointer Synchronization

3. Verify that the mouse and video have been properly configured during the installation process. Please refer to **Chapter 3: *Installation and Configuration*** (see "Installation and Configuration" on page 15) for complete instructions.
4. Force an auto-sense by clicking the Virtual KVM Client auto-sense button.
5. If that does not improve the mouse synchronization (for Linux, UNIX, and Solaris KVM target servers):
 - a. Open a terminal window.
 - b. Enter the `xset mouse 1 1` command.
 - c. Close the terminal window.
6. Click the Virtual KVM Client mouse synchronization  button.


Additional Notes for Intelligent Mouse Mode

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

Connection Menu

Properties Dialog

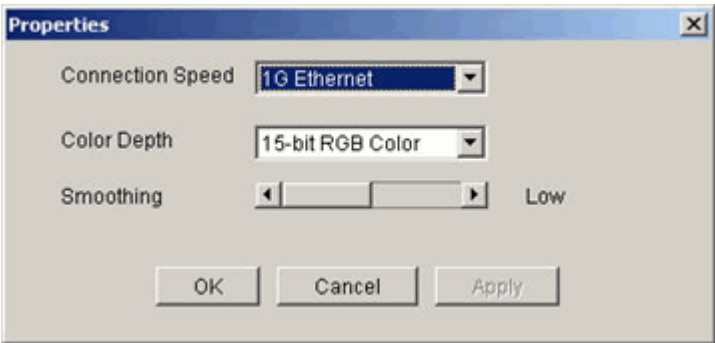
The Dominion KX II dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. Dominion KX II units optimize KVM output not only for LAN use, but also for WAN use. These units can also control color depth and limit video output, offering an optimal balance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

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

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

➤ *To set the connection properties:*

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



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

- Auto
- 1G Ethernet
- 100 Mb Ethernet
- 10 Mb Ethernet
- 1.5 Mb (MAX DSL/T1)
- 1 Mb (Fast DSL/T1)
- 512 Kb (Medium DSL/T1)

Connection Menu

384 Kb (Slow DSL/T1)

256 Kb (Cable)

128 Kb (Dual ISDN)

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

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

15-bit RGB Color

8-bit RGB Color

4-bit Color

4-bit Gray

3-bit Gray

2-bit Gray

Black and White

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

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

➤ *To cancel without saving changes:*

- Click Cancel.

Connection Info

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

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

The following information is displayed about the current connection:

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

➤ *To copy this information:*

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

Exit

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


- Choose Connection > Exit.

Keyboard Menu

Send Ctrl+Alt+Delete

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

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

	Send Ctrl+Alt+Delete	Sends a Ctrl+Alt+Delete key sequence to the target server
---	----------------------	---

➤ *To send a Ctrl+Alt+Delete key sequence to the target server:*

- Choose Keyboard > Send Ctrl+Alt+Delete, or
- Click the Send Ctrl+Alt+Delete button from toolbar

Keyboard Macros

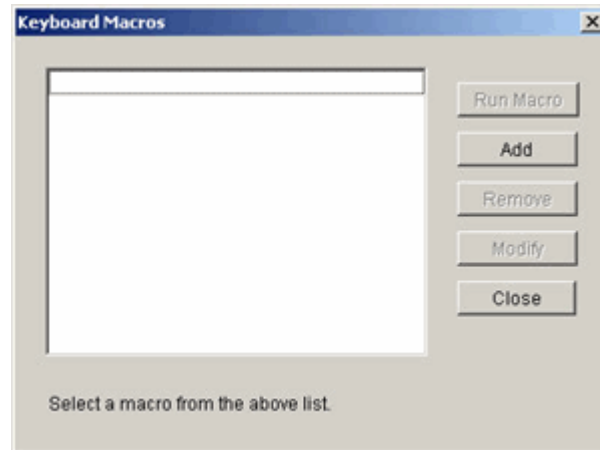
Keyboard macros ensure that keystroke combinations intended for the target server, are sent to and interpreted only by the target server. Otherwise, they might be interpreted by the computer on which the Virtual KVM Client is running (your client PC).

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

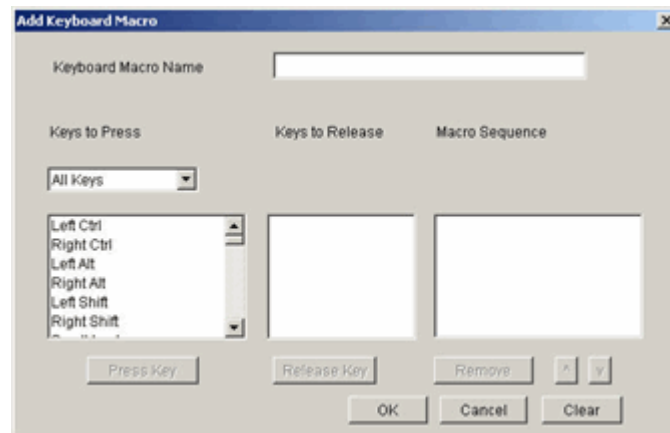
Creating a Keyboard Macro

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

1. Choose Keyboard > Keyboard Macros. The Keyboard Macros window opens:



2. Click Add. The Add Keyboard Macro window opens:



3. Type a name in the Keyboard Macro Name field. This is the name that will display on the Virtual KVM Client menu bar after the macro is created. In this example, type Minimize All Windows.
4. In the Keys to Press drop-down list:
 - a. Scroll through and select each key for which you would like to emulate a key press (in the order in which they are to be pressed).
 - b. Click the Press Key button after each selection. As each key is selected, it displays in the Keys to Release field.

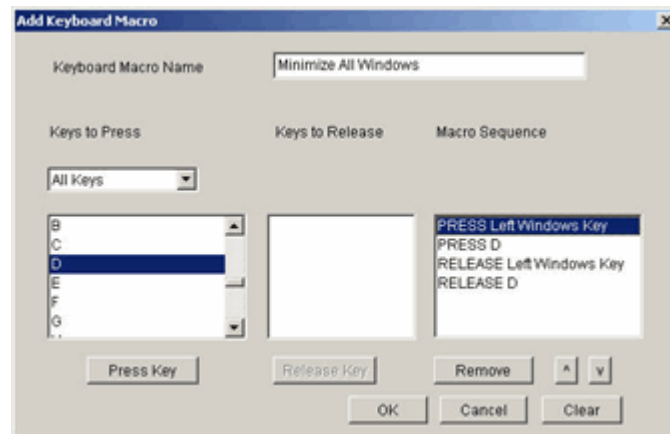
Keyboard Menu

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

5. In the Keys to Release field:
 - a. Choose each key for which you would like to emulate a key release (in the order in which they are to be released).
 - b. Click Release Key after each selection.

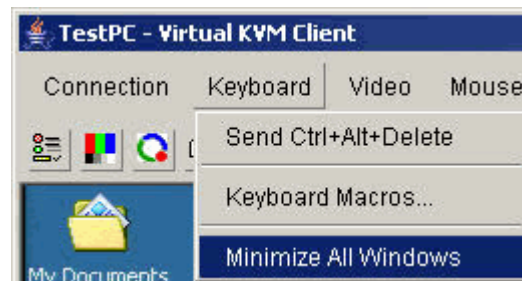
In this example, both keys pressed must also be released.

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



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

7. Click OK in the Add Keyboard Macro window to save the macro.
8. Click Close from the Keyboard Macros window. The keyboard macro created is now listed as an option from Keyboard menu:



➤ *To cancel without saving changes:*

- Click Cancel.

➤ *To clear all fields and start over:*

- Click the Clear button.

Running a Keyboard Macro

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

➤ *To execute a macro (using this example):*

- Choose Keyboard > Minimize All Windows.

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

➤ *To execute a macro:*

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

Modifying a Keyboard Macro

➤ *To modify a macro:*

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

Removing a Keyboard Macro

Please exercise caution in the removal of macros; you are not prompted to confirm their deletion.

Video Menu

➤ *To remove a macro:*

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

Video Menu

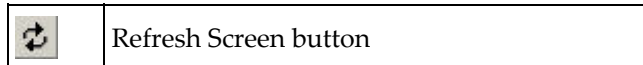
Video settings can be refreshed automatically in several ways:

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

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

Refresh Screen

The Refresh Screen option forces a refresh of the video screen. The entire video screen is redrawn.



➤ *To refresh the video settings:*

- Choose Video > Refresh Screen, or
- Click the Refresh Screen button from toolbar

Auto-sense Video Settings

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




➤ *To automatically detect the video settings:*

- Choose Video > Auto-sense Video Settings, or
- Click the Auto-Sense Video Settings button from toolbar

A message is displayed that auto adjustment is in progress.

Calibrate Color

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

	Calibrate Color	Adjusts color settings to optimize the video display.
---	-----------------	---


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

➤ *To calibrate the color:*

1. Open a remote KVM connection to any target server running a graphical user interface.
2. Choose Video > Calibrate Color (or click the Calibrate Color button). The target device screen updates its color calibration.

Video Settings

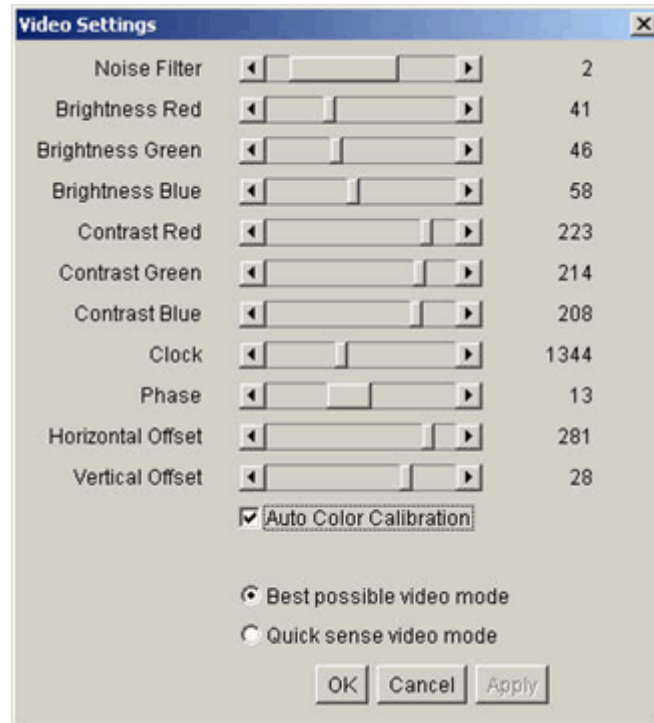
Use the Video Settings option to manually adjust the video settings.

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

Video Menu

➤ *To change the video settings:*

1. Choose Video > Video Settings. The Video Settings window opens displaying the current settings:



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

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

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

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

Mouse Menu

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

- *To cancel with saving your changes:*
 - Click Cancel.

Mouse Menu

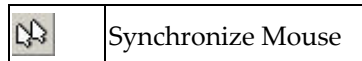
When controlling a target server, the Dominion KX II Remote Console displays two mouse cursors: one belonging to your client workstation and the other belonging to the target server. You can operate in either single mouse mode or dual mouse mode. When in dual mouse mode and properly configured, these two mouse cursors will align. If you experience difficulty with mouse synchronization, refer to ***Configure Target Servers*** (see "Step 1: Configure KVM Target Servers" on page 16).

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

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

Synchronize Mouse

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



- *To synchronize the mouse:*
 - Choose Mouse > Synchronize Mouse, or
 - Click the Synchronize Mouse button from the toolbar

Single Mouse Cursor

Single Mouse Cursor enters single mouse mode, in which only the target server mouse cursor is shown; the local PC mouse pointer no longer appears on-screen. While in single mouse mode, the Synchronize Mouse option is not available (there is no need to synchronize a single mouse cursor).

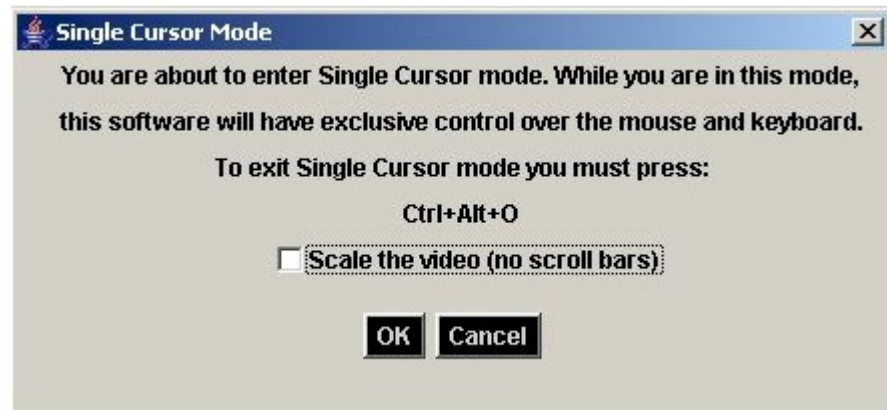


➤ *To enter single mouse mode:*

- Choose Mouse > Single Mouse Cursor, or
- Click the Single/Double Mouse Cursor button from the toolbar

➤ *To exit single mouse mode:*

1. When entering single mouse mode, the following message is displayed. Click OK.



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

Standard

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

➤ *To enter standard mouse mode:*

- Choose Mouse > Standard.

Intelligent

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

For additional information on Intelligent Mouse mode, refer to the Raritan Multi-Platform Client User Guide (Appendix B: Conditions for Intelligent Mouse Synchronization) available on Raritan's Website <http://www.raritan.com/support/productdocumentation>, or on the Raritan User Manuals & Quick Setup Guides CD ROM included with your Dominion KX II shipment.

- *To enter intelligent mouse mode:*
- Choose Mouse > Intelligent.

Absolute

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

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

- *To enter absolute mouse mode:*
- Choose Mouse > Absolute.

Virtual Media

Refer to the chapter on **Virtual Media** (on page 88) for complete information about setting up and using virtual media.

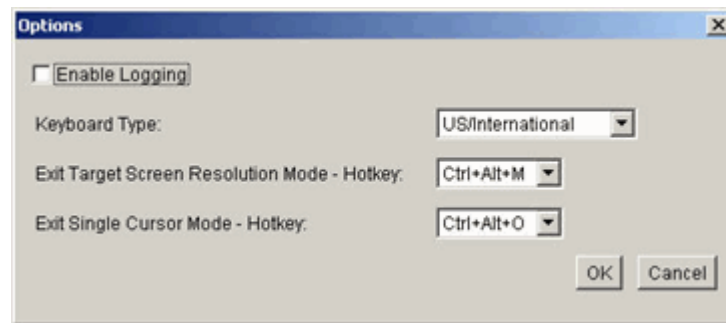
Tools Menu

Options

From the Tools menu, you can specify certain options for use with the Virtual KVM Client: synchronize mouse when in dual mouse mode, enable logging, keyboard type, and the exit target screen resolution mode hotkey.

➤ *To set the tools options:*

1. Choose Tools > Options. The Options window opens:



2. Select the Enable Logging checkbox only if directed to by Technical Support. This option creates a log file in your home directory.
3. Choose the Keyboard Type from the drop-down list (if necessary). The options include:
 - US/International
 - French (France)
 - German (Germany)
 - Japanese
 - United Kingdom
 - Korean (Korea)
 - Traditional and Simplified Chinese
 - German
 - Belgian
 - Norwegian
 - Danish
 - Swedish

View Menu

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

View Menu

View Toolbar

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

- *To toggle the display of the toolbar (on and off):*
 - Choose View > View Toolbar.

Scaling

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

- *To toggle scaling (on and off):*
 - Choose View > Scaling.

Target Screen Resolution

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

- *To enter target screen resolution:*
 - Choose View > Target Screen Resolution.
- *To exit target screen resolution mode:*
 - Press the hotkey configured in the Tools Options dialog. The default is Ctrl+Alt+M.

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

Help Menu

About Raritan Virtual KVM Client

This menu option provides version information about the Virtual KVM Client should you require assistance from Raritan technical support.

- *To obtain version information:*
 - Choose Help > About Raritan Virtual KVM Client.

Chapter 7 Virtual Media

In This Chapter

- Overview.....89
- Prerequisites for Using Virtual Media91
- Using Virtual Media92
- Opening a KVM Session93
- Connecting to Virtual Media.....94
- Disconnecting Virtual Media97
- File Server Setup (File Server ISO Images Only)98

Overview

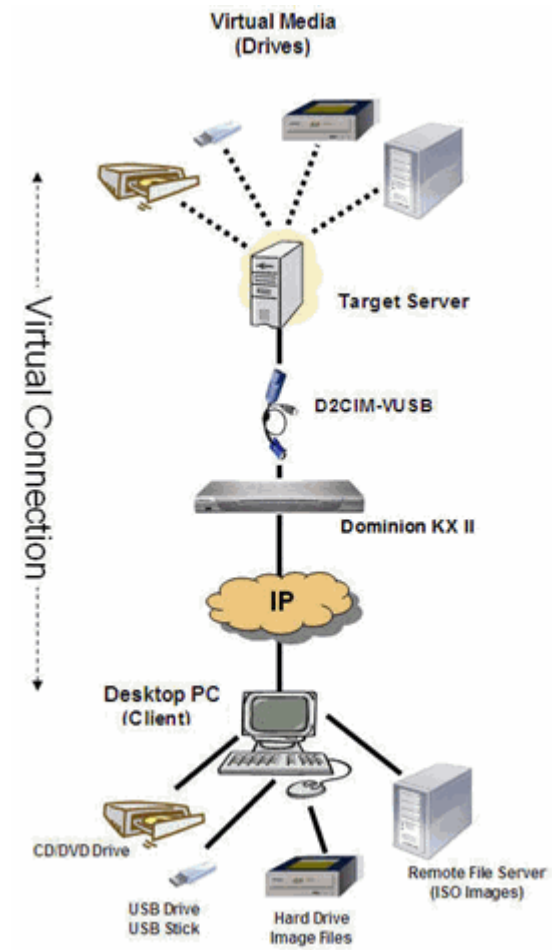
Virtual media extends KVM capabilities by enabling KVM target servers to remotely access media from the client PC and network file servers. With this feature, media mounted on the client PC and network file servers is essentially mounted virtually by the target server. The target server can then read from and write to that media as if it were physically connected to the target server itself. Virtual media can include internal and USB-mounted CD and DVD drives, USB mass storage devices, PC hard drives, and ISO images (disk images).

Virtual media provides the ability to perform additional tasks remotely, such as:

- transferring files
- running diagnostics
- installing or patching applications
- complete installation of the operating system

This expanded KVM control eliminates most trips to the data center, saving time and money, thereby making virtual media very powerful.

Overview



Prerequisites for Using Virtual Media

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

Dominion KX II

- For users requiring access to virtual media, Dominion KX II permissions must be set to allow access to the relevant ports, as well as virtual media access (VM Access port permission) for those ports. Port permissions are set at the group-level; please refer to *Setting Port Permissions* (on page 110) for more information.
- (Optional) If you want to use PC-Share, *VM Share Mode* (see "Encryption & Share" on page 157) must also be enabled in the Security Settings page.

Client PC

- Certain virtual media options require administrative privileges on the client PC (e.g., drive redirection of complete drives).

Note: If you are using Microsoft Vista, turn User Account Control off: Control Panel > User Accounts > User Account Control > turn off.

If you would prefer not to change Vista account permissions, run Internet Explorer as an administrator. To do this, click on the Start Menu, locate IE, right click it and select Run as Administrator.

- USB 2.0 ports are both faster and preferred.

Target Server

- KVM target servers must support USB connected drives.
- KVM target servers running Windows 2000 must have all of the recent patches installed.

Using Virtual Media

With the Dominion KX II virtual media feature, you can mount up to two drives (of different types). These drives are accessible for the duration of the KVM session.

For example, you can mount a specific CD-ROM, use it, and then disconnect it when you are done. The CD-ROM virtual media “channel” will remain open, however, so that you can virtually mount another CD-ROM. These virtual media “channels” remain open until the KVM session is closed.

➤ *To use virtual media:*

1. Connect/attach the media to the client or network file server that you want to access from the target server. This need not be the first step, but it must be done prior to attempting to access this media.
2. Verify that the appropriate *prerequisites* (see "Prerequisites for Using Virtual Media" on page 91) are met.
3. (File server ISO images only) If you plan to access file server ISO images, identify those file servers and images through the Dominion KX II Remote Console *File Server Setup page* (see "File Server Setup (File Server ISO Images Only)" on page 98).

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

4. *Open a KVM session* (see "Opening a KVM Session" on page 93) with the appropriate target server.
5. Connect to the virtual media.

For:	Select this VM option:
Local drives	Connect Drive (see "Local Drives" on page 94)
Local CD/DVD drives	Connect CD-ROM/ISO Image (see "CD-ROM/DVD-ROM/ISO Images" on page 96)
ISO Images	Connect CD-ROM/ISO Image
File Server ISO Images	Connect CD-ROM/ISO Image

6. Upon completion of your tasks, *disconnect the virtual media* (see "Disconnecting Virtual Media" on page 97).

Opening a KVM Session

➤ *To open a KVM session:*

1. Open the Port Access page from the Dominion KX II Remote Console.
2. Connect to the target server from the Port Access page:
 - a. Click the Port Name for the appropriate server.
 - b. Choose the Connect option from the Port Action Menu.

The target server opens in a *Virtual KVM Client* (on page 65) window.

Connecting to Virtual Media

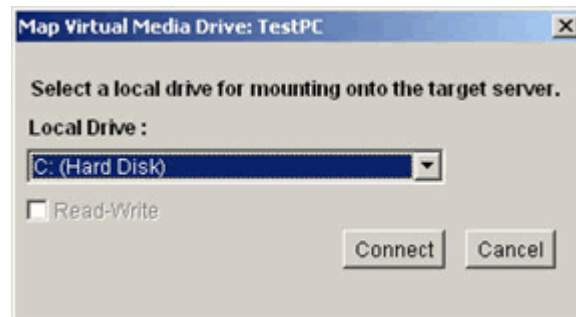
Local Drives

This option mounts an entire drive; the entire disk drive is mounted virtually onto the target server. Use this option for hard drives and external drives only; it does not include network drives, CD-ROM, or DVD-ROM drives. This is the only option for which Read-Write is available.

Note: KVM target servers running certain version of the Windows operating system may not accept new mass storage connections after an NTFS-formatted partition (e.g., the local C drive) has been redirected to them. If this occurs, close the Dominion KX II Remote Console and reconnect before redirecting another virtual media device. If other users are connected to the same target server, they must also close their connections to the target server.

➤ *To access a drive on the client computer:*

1. From the Virtual KVM Client, select Virtual Media > Connect Drive.
The Map Virtual Media Drive dialog opens:



2. Choose the drive from the Local Drive drop-down list.
3. If you want read and write capabilities, select the Read-Write option checkbox. This option is disabled for non-removable drives. Please refer to the *conditions when read-write is not available* (on page 95) for more information. When checked, you will be able to read or write the connected USB disk.

WARNING: Enabling Read-Write access can be dangerous! Simultaneous access to the same drive from more than one entity can result in data corruption. If you do not require write access, leave this option unselected.

4. Click Connect. The media will be mounted on the target server virtually. You can access the media just like any other drive.

Note: If there is no USB connection to the target server, you will see a warning message that says, "The virtual media capability is set up but will not be available until the USB cable is connected or the target is powered on. Please check your USB connectivity or see if the target is powered on." Resolve this issue, then connect to the drive again.

Conditions when Read-Write is not Available

Virtual media read-write is not available in the following situations:

- For all hard drives.
- When the drive is write-protected.
- When the user does not have read-write permission:
 - Port Permission Access is set to None or View
 - Port Permission VM Access is set to Read-Only or Deny

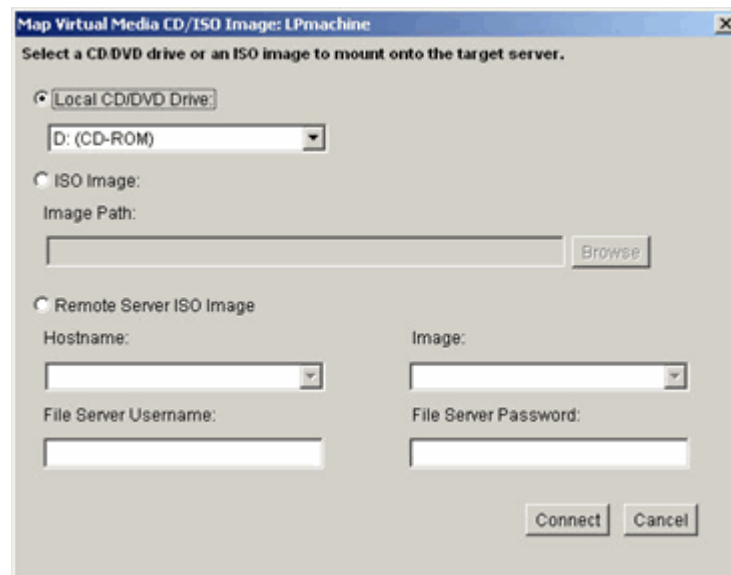
CD-ROM/DVD-ROM/ISO Images

This option mounts CD-ROM, DVD-ROM, and ISO images.

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

➤ To access a CD-ROM, DVD-ROM, or ISO image:

1. From the Virtual KVM Client, choose Virtual Media > Connect CD-ROM/ISO Image. The Map Virtual Media CD/ISO Image dialog opens:



2. For internal and external CD-ROM or DVD-ROM drives:
 - a. Choose the Local CD/DVD Drive option.
 - b. Choose the drive from the Local CD/DVD Drive drop-down list. All available internal and external CD and DVD drive names will be populated in the drop-down list.
 - c. Click Connect.
3. For ISO images:
 - a. Choose the ISO Image option. Use this option when you want to access a disk image of a CD, DVD, or hard drive. ISO format is the only format supported.
 - b. Click the Browse button.
 - c. Navigate to the path containing the disk image you want to use and click Open. The path is populated in the Image Path field.

- d. Click Connect.
4. For remote ISO images on a file server:
 - a. Choose the Remote Server ISO Image option.
 - b. Choose Hostname and Image from the drop-down lists. The file servers and image paths available are those that you configured using the File Server Setup page. Only items you configured using the Dominion KX II File Server Setup page will be in the drop-down list.
 - c. File Server Username. Username required for access to the file server.
 - d. File Server Password. Password required for access to the file server (field is masked as you type).
 - e. Click Connect.

The media will be mounted on the target server virtually. You can access the media just like any other drive.

Disconnecting Virtual Media

- *To disconnect the Virtual Media drives:*
- For local drives, choose Virtual Media > Disconnect Drive.
 - For CD-ROM, DVD-ROM, and ISO images, choose Virtual Media > Disconnect CD-ROM/ISO Image.

Note: In addition to disconnecting the virtual media using the Disconnect option, simply closing the KVM connection closes the Virtual Media as well.

File Server Setup (File Server ISO Images Only)

Note: This feature is only required when using virtual media to access file server ISO images.

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

Use the Dominion KX II Remote Console File Server Setup page to designate the files server(s) and image paths that you want to access using Dominion KX II Virtual Media. File server ISO image(s) specified here will become available for selection in the Remote Server ISO Image Hostname and Image drop-down lists (in the **Map Virtual Media CD/ISO Image dialog** (see "CD-ROM/DVD-ROM/ISO Images" on page 96)).

➤ *To designate file server ISO images for virtual media access:*

1. Choose Virtual Media from the Dominion KX II Remote Console. The File Server Setup page opens:

Selected	Host Name/IP Address	Image Path
<input checked="" type="checkbox"/>	192.168.1.193	/Images/disk1.iso
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

Save Cancel

2. Enter information about the file server ISO images that you want to access:

- Host Name/IP Address. Host name or IP Address of the file server.
 - Image Path. Full path name of the location of the ISO image.
3. Select the Selected checkbox for all media that you want accessible as virtual media.
 4. Click Save. All media specified here will now be available for selection in the Map Virtual Media CD/ISO Image dialog.
- *To cancel without saving:*
- Click Cancel.

Chapter 8 User Management

In This Chapter

User Management Menu	100
User List	101
Add New User	102
User Group List.....	104
Add a New User Group (Shared).....	105
Add New User Group.....	107
Change Password	114
Authentication Settings.....	115

User Management Menu

The User Management menu is organized as follows: User List, Add New User, User Group List, Add New User Group, Change Password, and Authentication Settings.

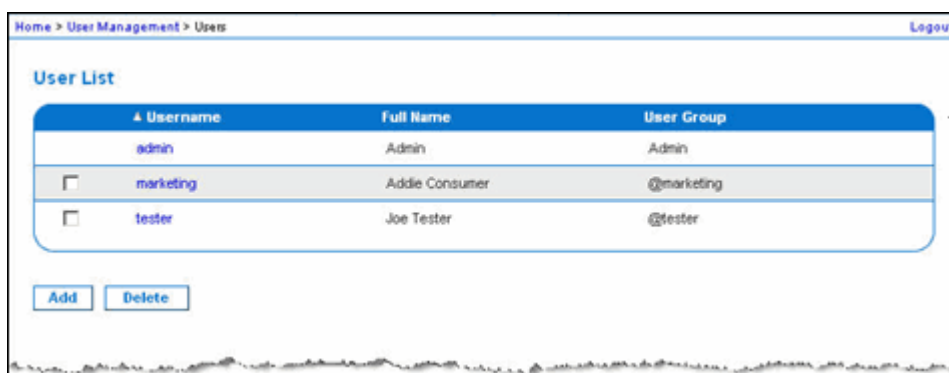
Use:	To:
User List	Display an alphabetical list of all users; add, modify, or delete users.
Add New User	Add new users; modify user information.
User Group List	Display an alphabetical list of all user groups; add, modify, or delete user groups.
Add New User Group	Add new user groups; modify user group information.
Change Password	Change password for a specific user.
Authentication Settings	Configure the type of authentication used for access to the Dominion KX II.

User List

The User List page displays a list of all users including their Username, Full Name, and User Group. The list can be sorted on any of the columns by clicking on the column name. From the User List page, you can also add, modify, or delete users.

➤ *To view the list of users:*

- Choose User Management > User List. The User List page opens:



➤ *To add a new user:*

- Click the Add button. The User page opens. For complete information about the User page, refer to **Add New User** (on page 102).

➤ *To modify an existing user:*

1. Locate the user from among those listed.
2. Click on the Username. The User page opens. For complete information editing the user, refer to **Modify Existing User** (on page 103).

➤ *To delete a user:*

1. Select the user from among those listed by selecting the checkbox to the left of the Username.
2. Click Delete. You are prompted to confirm the deletion.
3. Click OK.

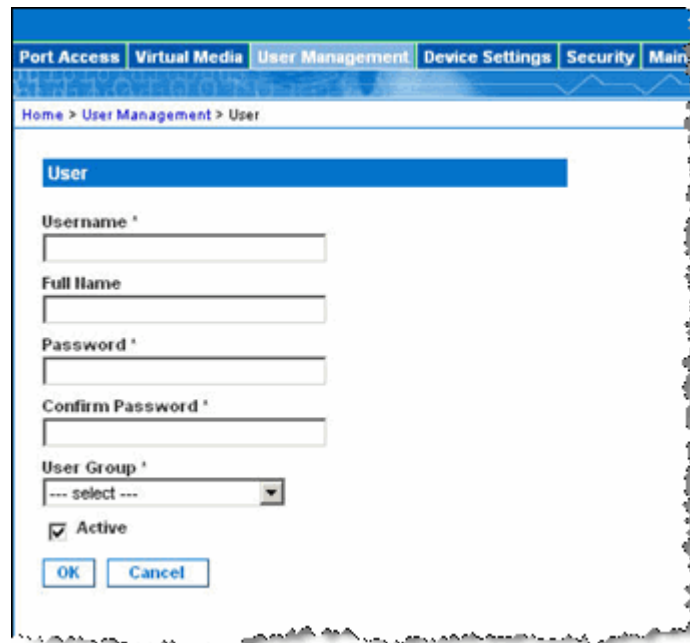
Add New User

It is a good idea to define user groups before creating Dominion KX II users, because when you add a user, you must assign that user to an existing user group. From the **User** page, you can add new users, modify user information, and reactivate users that have been deactivated.

*Note: A username can be deactivated (Active checkbox is deselected when the number of failed login attempts has exceeded the maximum login attempts set in the Security Settings page. Refer to **Security Settings** (on page 153) for more information.*

➤ To add a new user:

1. Open the User page using one of these methods:
 - Choose User Management > Add New User, or
 - Click the Add button from the User List page

The screenshot shows a web interface for adding a new user. At the top, there is a navigation bar with tabs: Port Access, Virtual Media, User Management (selected), Device Settings, Security, and Main. Below the navigation bar, a breadcrumb trail reads 'Home > User Management > User'. The main content area is titled 'User' and contains several input fields: 'Username *', 'Full Name', 'Password *', 'Confirm Password *', and 'User Group *' (a dropdown menu with '--- select ---' as the current selection). There is also a checkbox labeled 'Active' which is checked. At the bottom of the form are 'OK' and 'Cancel' buttons.

2. Type a unique name in the Username field (up to 16 characters).
3. Type the person's full name in the Full Name field (up to 64 characters).
4. Type a password in the Password field; retype the password in the Confirm Password field (up to 64 characters).

5. Choose the group from the User Group drop-down list. The list contains all groups you have created in addition to the system-supplied default groups (<Unknown> (default setting), Admin, Individual Group). If you do not want to associate this user with an existing User Group, choose Individual Group from the drop-down list.

Note: The Admin user must be a member of the Admin group.

For more information about permissions for an Individual Group, refer to *Set Permissions for Individual Group* (on page 114).

6. To activate this user, select the Active checkbox. The default is activated (enabled).
7. Click OK.

Modify Existing User

➤ *To modify an existing user:*

1. In the User page, change the appropriate fields. (Refer to *Add New User* (on page 102) for information about how to get access the User page.)
2. Click OK.

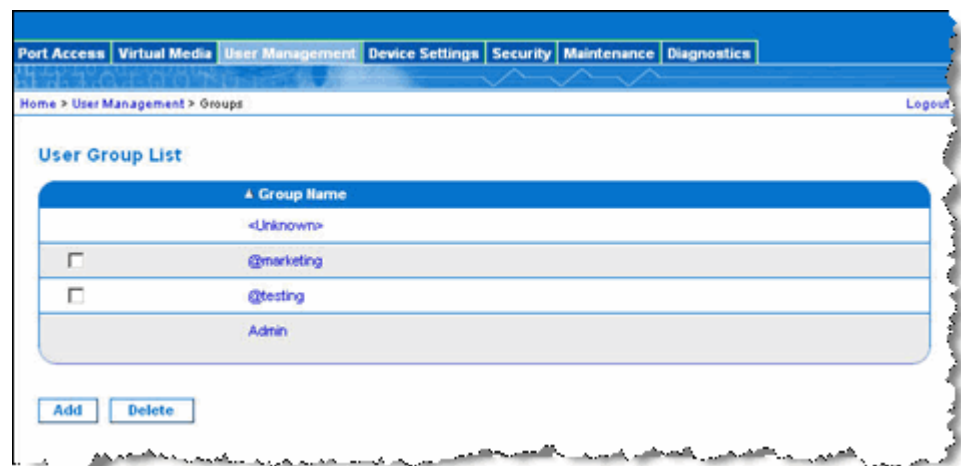
User Group List

User groups are used with local and remote authentication (via RADIUS or LDAP/LDAPS). It is a good idea to define user groups before creating individual users, because when you add a user, you must assign that user to an existing user group.

The User Group List page displays a list of all user groups, which can be sorted in ascending or descending order by clicking on the Group Name column heading. From the User Group List page, you can also add, modify, or delete user groups.

➤ *To list the user groups:*

- Choose User Management > User Group List. The User Group List page opens:



➤ *To add a new user group:*

- Click the Add button. The Group page opens. For complete information about the Group page, refer to **Add New User Group** (on page 107).

➤ *To modify an existing user group:*

1. Locate the user group from among those listed.
2. Click on the Group Name. The Group page opens. For complete information editing the group, refer to **Modify Existing User Group** (on page 113).

➤ *To delete a user group:*

Important: If you delete a group with users in it, the users are automatically assigned to the <unknown> user group.

Tip: To determine the users belonging to a particular group, sort the User List by User Group.

1. Choose a group from among those listed by checking the checkbox to the left of the Group Name.
2. Click Delete.
3. When prompted to confirm the deletion, click OK.

Add a New User Group (Shared)

➤ *To add a new user group:*

1. Open the Group page using one of these methods:
 - Choose User Management > Add New User Group, or

Add a New User Group (Shared)

- Click the Add button from the User Group List page

Home > User Management > Group

Group

Group Name *

Permissions

☐ Device Settings
☐ Diagnostics
☐ Maintenance
☐ PC-Share
☐ Security
☐ User Management

Port Permissions

Port	Access	VM Access	Power Control
Dominion-ICQ_Port1	None	Deny	Deny
Dominion-ICQ_Port2	None	Deny	Deny
Dominion-ICQ_Port3	None	Deny	Deny
Dominion-ICQ_Port4	None	Deny	Deny
charles_cim-renamed	None	Deny	Deny
Dominion-ICQ_Port6	None	Deny	Deny
idcim-rusb-win2k-rev	None	Deny	Deny
Dominion-ICQ_Port8	None	Deny	Deny
Dominion-ICQ_Port9	None	Deny	Deny
Dominion-ICQ_Port10	None	Deny	Deny
Dominion-ICQ_Port11	None	Deny	Deny
Dominion-ICQ_Port12	None	Deny	Deny
Dominion-ICQ_Port13	None	Deny	Deny
Dominion-ICQ_Port14	None	Deny	Deny
Dominion-ICQ_Port15	None	Deny	Deny
Dominion-ICQ_Port16	None	Deny	Deny
Dominion-ICQ_Port17	None	Deny	Deny
Dominion-ICQ_Port18	None	Deny	Deny
Dominion-ICQ_Port19	None	Deny	Deny
Dominion-ICQ_Port20	None	Deny	Deny
Dominion-ICQ_Port21	None	Deny	Deny
Dominion-ICQ_Port22	None	Deny	Deny
Dominion-ICQ_Port23	None	Deny	Deny
Dominion-ICQ_Port24	None	Deny	Deny
Dominion-ICQ_Port25	None	Deny	Deny
Dominion-ICQ_Port26	None	Deny	Deny
Dominion-ICQ_Port27	None	Deny	Deny
Dominion-ICQ_Port28	None	Deny	Deny
Dominion-ICQ_Port29	None	Deny	Deny
Dominion-ICQ_Port30	None	Deny	Deny
Dominion-ICQ_Port31	None	Deny	Deny
Dominion-ICQ_Port32	None	Deny	Deny

☐ Set All to None ☐ Set All VM Access to Deny ☐ Set All Power to Deny
☐ Set All to View ☐ Set All VM Access to Read-Only ☐ Set All Power to Access
☐ Set All to Control ☐ Set All VM Access to Read-Write

IP ACL

Rule # Starting IP Ending IP Action

 ACCEPT

Append Insert Replace Delete

OK Cancel

Copyright © 2007 Raritan Computer Inc.

The Group page is organized into the following categories: Group, Permissions, Port Permissions, and IP ACL.

- Type a descriptive name for the new user group into the Group Name field.

3. Set the Permissions for the group. Select the checkboxes before the permissions you want to assign to all of the users belonging to this group. Refer to Setting Permissions for more information.
4. Set the Port Permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). Refer to *Setting Port Permissions* (on page 110) for more information.
5. **Set the IP ACL** (see "Group-based IP ACL (Access Control List)" on page 110) (optional). This feature limits access to the Dominion KX II device by specifying IP addresses; it applies only to users belonging to a specific group, unlike the *IP Access Control* (on page 160) list feature which applies to all access attempts to the device (and takes priority).
6. Click OK.

Note: Several administrative functions are available within MPC and from the Dominion KX II Local Console; these functions are available only to members of the default ADMIN group.

Add New User Group

- *To add a new user group:*
1. Open the Group page using one of these methods:
 - Choose User Management > Add New User Group, or

Add New User Group

- Click the Add button from the User Group List page

Home > User Management > Group Logout

Group

Group Name ^

▼ Permissions

☐ Device Settings
☐ Diagnostics
☐ Maintenance
☐ Modem Access
☐ PC-Share
☐ Security
☐ User Management

▼ Port Permissions

Port	Access	VM Access	Power Control
Win Target	Deny ▼	Deny ▼	Deny ▼
Dominion_KSX2_Port2	Deny ▼	Deny ▼	Deny ▼
Dominion_KSX2_Port3	Deny ▼	Deny ▼	Deny ▼
KSX-G2 Admin	Deny ▼	Deny ▼	Deny ▼
Dominion_KSX2_Port5	Deny ▼	Deny ▼	Deny ▼
Dominion_KSX2_Port6	Deny ▼	Deny ▼	Deny ▼
Dominion_KSX2_Port7	Deny ▼	Deny ▼	Deny ▼
Dominion_KSX2_Port8	Deny ▼	Deny ▼	Deny ▼
Cisco 2501	Deny ▼		Deny ▼
SP-2	Deny ▼		Deny ▼
Serial Port 3	Deny ▼		Deny ▼
Serial Port 4	Deny ▼		Deny ▼
SP - 5	Deny ▼		Deny ▼
Serial Port 6	Deny ▼		Deny ▼
Serial Port 7	Deny ▼		Deny ▼
Serial Port 8	Deny ▼		Deny ▼

☐ Set All to Deny
☐ Set All to View
☐ Set All to Control

☐ Set All VM Access to Deny
☐ Set All VM Access to Read-Only
☐ Set All VM Access to Read-Write

☐ Set All Power to Deny
☐ Set All Power to Access

▼ IP ACL

Rule #	Starting IP	Ending IP	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	ACCEPT ▼

Copyright © 2007 Raritan Computer Inc.

The Group page is organized into the following categories: Group, Permissions, Port Permissions, and IP ACL.

- Type a descriptive name for the new user group into the Group Name field.

3. Set the Permissions for the group. Select the checkboxes before the permissions you want to assign to all of the users belonging to this group. Refer to Setting Permissions for more information.
4. Set the Port Permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). Refer to *Setting Port Permissions* (on page 110) for more information.
5. **Set the IP ACL** (see "Group-based IP ACL (Access Control List)" on page 110) (optional). This feature limits access to the Dominion KX II device by specifying IP addresses; it applies only to users belonging to a specific group, unlike the *IP Access Control* (on page 160) list feature which applies to all access attempts to the device (and takes priority).
6. Click OK.

Note: Several administrative functions are available within MPC and from the Dominion KX II Local Console; these functions are available only to members of the default ADMIN group.

Setting Permissions

Important: Selecting the User Management checkbox allows the members of the group to change the permissions of all users, including their own. Carefully consider granting these permissions.

Permission	Description
Device Settings	Network settings, date/time settings, port configuration (channel names, power associations), event management (SNMP, Syslog), virtual media file server setup.
Diagnostics	Network interface status, network statistics, ping host, trace route to host, Dominion KX II diagnostics.
Maintenance	Backup and restore database, firmware upgrade, factory reset, reboot.
PC-Share	Simultaneous access to the same target by multiple users.
Security	SSL certificate, security settings (VM Share, PC-Share), IP ACL.
User Management	User and group management, remote authentication (LDAP/RADIUS), login settings.

Setting Port Permissions

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

Access		VM Access		Power Control	
Option	Description	Option	Description	Option	Description
None*	Denied access completely	Deny*	Virtual media permission is denied altogether for the port	Deny*	Denied access completely
View	View the video (but not interact with) the connected target server	Read-Only	Virtual media access is limited to read access only	Access	Complete access
Control	Control the connected target server	Read-Write	Complete access (read, write) to virtual media		

* Default setting

Tip: Use the checkboxes to quickly set all the permissions the same for every port.

Group-based IP ACL (Access Control List)

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

This feature limits access to the Dominion KX II device by users in the selected group to specific IP addresses. This feature applies only to users belonging to a specific group, unlike the IP Access Control List feature which applies to all access attempts to the device, is processed first, and takes priority. Refer to *IP Access Control* (on page 160) for more information.

Important: The IP Address 127.0.0.1 is used by the Dominion KX II Local Port and cannot be blocked.

Use the IP ACL section of the Group page to add, insert, replace, and delete IP access control rules on a group-level basis.

Rule #	Starting IP	Ending IP	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	ACCEPT

Append Insert Replace Delete

➤ *To add (append) rules:*

1. Type the starting IP Address in the Starting IP field.
2. Type the ending IP Address in the Ending IP field.
3. Choose the Action from the available options:
 - Accept. IP Addresses specifying accept are allowed access to the Dominion KX II device.
 - Drop. IP Addresses specifying drop are denied access to the Dominion KX II device.
4. Click Append. The rule is added to the bottom of the rules list.
5. Repeat steps 1 through 4 for each rule you want to enter.

➤ *To insert a rule:*

1. Type a Rule #. A Rule # is required when using the Insert command.
2. Type the Starting IP and Ending IP fields.
3. Choose the Action from the drop-down list.
4. Click Insert. If the Rule # you just typed equals an existing Rule #, the new rule is placed ahead of the exiting rule and all rules are moved down in the list.

➤ *To replace a rule:*

1. Specify the Rule # you want to replace.

Add New User Group

2. Type the Starting IP and Ending IP fields.
3. Choose the Action from the drop-down list.
4. Click Replace. Your new rule replaces the original rule with the same Rule #.

➤ *To delete a rule:*

1. Specify the Rule # you want to delete.
2. Click Delete.
3. When prompted to confirm the deletion, click OK.

Important: ACL rules are evaluated in the order in which they are listed. For instance, in the example shown here, if the two ACL rules were reversed, Dominion would accept no communication at all.

IP ACL			
Rule #	Starting IP	Ending IP	Action
1	192.168.50.1	192.168.55.255	ACCEPT
2	0.0.0.0	255.255.255.255	DROP
<input type="text"/>	<input type="text"/>	<input type="text"/>	ACCEPT ▾
<div>Append Insert Replace Delete</div>			

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

Modify Existing User Group

Note: All permissions are enabled (and cannot be changed) for the Admin group.

➤ To modify an existing user group:

1. From the Group page, change the appropriate fields and set the appropriate permissions.

Home > User Management > Group

Group

Group Name *

Permissions

☐ Device Settings
☐ Diagnostics
☐ Maintenance
☐ PC-Share
☐ Security
☐ User Management

Port Permissions

Port	Access	VM Access	Power Control
Dominion_KX2_101_Port1	Deny	Deny	Deny
Power Port 1	Deny		Deny

IP ACL

Rule #	Starting IP	Ending IP	Action
			ACCEPT

Append Insert Replace Delete

OK Cancel

2. Set the Permissions for the group. Select the checkboxes before the permissions you want to assign to all of the users belonging to this group. Refer to *Setting Permissions* for more information.
3. Set the Port Permissions. Specify the server ports that can be accessed by users belonging to this group (and the type of access). Refer to *Setting Port Permissions* (on page 110) for more information.
4. Set the IP ACL (optional). This feature limits access to the Dominion KX II device by specifying IP addresses. Refer to *Group-based IP Access Control List* (see "Group-based IP ACL (Access Control List)" on page 110) for more information.
5. Click OK.

Change Password

Set Permissions for Individual Group

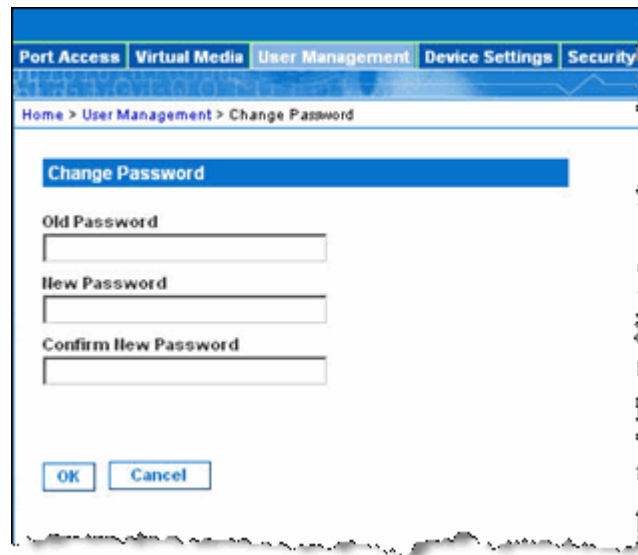
➤ *To set permissions for an individual user group:*

1. Locate the user from among the groups listed. Individual groups can be identified by the @ in the Group Name.
2. Click the Group Name. The Group page opens.
3. Select the appropriate permissions.
4. Click OK.

Change Password

➤ *To change your password:*

1. Choose User Management > Change Password. The Change Password page opens:

A screenshot of a web application interface for changing a password. At the top, there is a navigation bar with tabs: 'Port Access', 'Virtual Media', 'User Management' (which is selected), 'Device Settings', and 'Security'. Below the navigation bar, a breadcrumb trail reads 'Home > User Management > Change Password'. The main content area has a title 'Change Password' in a blue box. Below the title are three text input fields labeled 'Old Password', 'New Password', and 'Confirm New Password'. At the bottom of the form are two buttons: 'OK' and 'Cancel'.

2. Type your current password in the Old Password field.
3. Type a new password in the New Password field; retype the new password in the Confirm New Password field. Passwords can be up to 64 characters in length and can consist of English alphanumeric characters and *special characters* (see "Valid Special Characters" on page 33).
4. Click OK.
5. You will receive confirmation that the password was successfully changed. Click OK.

*Note: If strong passwords are in use, this page displays information about the format required for the passwords. For more information about passwords and strong passwords, refer to **Security Settings - Strong Passwords** (see "Strong Passwords" on page 155).*

Authentication Settings

From the Authentication Settings page you can configure the type of authentication used for access to your Dominion KX II. Refer to **Authentication vs. Authorization** (on page 38) for more information about how authentication and authorization operate and differ.

Note: Even if you select remote authentication (LDAP or RADIUS), local authentication is still used.

➤ *To configure authentication:*

1. Choose User Management > Authentication Settings. The Authentication Settings page opens:

The screenshot displays the 'Authentication Settings' page. At the top, there are tabs for 'Port Access', 'Virtual Media', 'User Management', 'Device Settings', and 'Security'. Below these is a breadcrumb trail: 'Home > User Management > Authentication Settings'. The main heading is 'Authentication Settings'. There are three radio buttons for selecting the authentication method: 'Local Authentication' (selected), 'LDAP', and 'RADIUS'. Under the 'LDAP' section, the following fields are visible: 'Primary LDAP Server', 'Secondary LDAP Server', 'Secret Phrase', 'Confirm Secret Phrase', a checkbox for 'Enable Secure LDAP', 'Port' (set to 389), 'Secure LDAP Port' (set to 636), 'Certificate File' (with a 'Browse' button), 'DN of Administrative User', 'User Search DN', 'Type of External LDAP Server' (a dropdown menu set to 'Generic LDAP server'), 'Active Directory Domain', 'Primary RADIUS Server', 'Shared Secret', 'Authentication Port' (set to 1812), and 'Accounting Port' (set to 1813).

Authentication Settings

2. Choose the option for the authentication protocol you want to use (Local Authentication, LDAP, or RADIUS). Choosing the LDAP option enables the remaining LDAP fields; selecting the RADIUS option enables the remaining RADIUS fields.
3. If you choose Local Authentication, proceed to step 6.
4. If you choose LDAP, read the section entitled ***Implementing LDAP Remote Authentication*** (on page 116) for information about completing the fields in the LDAP section of the Authentication Settings page.
5. If you choose RADIUS, read the section entitled ***Implementing RADIUS Remote Authentication*** (on page 120) for information about completing the fields in the RADIUS section of the Authentication Settings page.
6. Click OK to save.

➤ *To cancel without saving changes:*

- Click Cancel.

➤ *To return to factory defaults:*

- Click the Reset to Defaults button.

Implementing LDAP Remote Authentication

Lightweight Directory Access Protocol (LDAP/LDAPS) is a networking protocol for querying and modifying directory services running over TCP/IP. A client starts an LDAP session by connecting to an LDAP/LDAPS server (the default TCP port is 389). The client then sends operation requests to the server, and the server sends responses in turn.

Reminder: Microsoft Active Directory functions natively as an LDAP/LDAPS authentication server.

➤ *To use the LDAP authentication protocol, enter the following information:*

1. Type the IP Address or DNS name of your LDAP/LDAPS remote authentication server in the Primary LDAP Server field. When the Enable Secure LDAP option is selected, the DNS name must be used.
2. (Optional) Type the IP Address or DNS name of your backup LDAP/LDAPS server in the Secondary LDAP Server field. When the Enable Secure LDAP option is selected, the DNS name must be used. Please note that the remaining fields share the same settings with the Primary LDAP Server field.

3. Type the server secret (password) required to authenticate against your remote authentication server in the Secret Phrase field and again in the Confirm Secret Phrase field. Enter the password in use on the LDAP/LDAPS server.
4. Dialback Query String. Type the dialback query string. If you are using Microsoft Active Directory, you must enter the following string:

msRADIUSCallbackNumber

Note: This string is case sensitive.

5. Select the Enable Secure LDAP checkbox if you would like to use SSL; the Secure LDAP Port field is enabled. Secure Sockets Layer (SSL) is a cryptographic protocol which allows Dominion KX II to communicate securely with the LDAP/LDAPS server.
6. The default Port is 389. Either use the standard LDAP TCP port or specify another port.
7. The default Secure LDAP Port is 636. Either use the default port or specify another port. This field is enabled when the Enable Secure LDAP checkbox is selected.
8. Certificate File. Consult your authentication server administrator to get the CA certificate file in Base64 encoded X-509 format for the LDAP/LDAPS server. Use the Browse button to navigate to the certificate file. This field is enabled when the Enable Secure LDAP option is selected.
9. DN of administrative User. Distinguished Name of administrative user; consult your authentication server administrator for the appropriate values to type into this field. An example DN of administrative User value might be:
"cn=Administrator,cn=Users,dc=testradius,dc=com".
10. User Search DN. This describes the name you want to bind against the LDAP/LDAPS, and where in the database to begin searching for the specified Base DN. An example Base Search value might be:
"cn=Users,dc=raritan,dc=com". Consult your authentication server administrator for the appropriate values to enter into these fields.
11. Type of external LDAP/LDAPS server. Choose from among the options available:
 - Generic LDAP Server.
 - Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.

12. Active Directory Domain. Type the name of the Active Directory Domain.

Returning User Group Information from Active Directory Server

The Dominion KX II supports user authentication to Active Directory (AD) without requiring that users be defined locally on the Dominion KX II. This allows Active Directory user accounts and passwords to be maintained exclusively on the AD server. Authorization and AD user privileges are controlled and administered through the standard Dominion KX II policies and user group privileges (that are applied locally to AD user groups).

*Note: If you are an existing Raritan, Inc. customer, and have already configured the Active Directory server by changing the AD schema, Dominion KX II still supports this configuration, and you do not need to perform the following operations. Please refer to **Appendix B: Updating the LDAP/LDAPS Schema** (see "Updating the LDAP Schema" on page 203) for information about updating the AD LDAP/LDAPS schema.*

- *To enable your AD server on the Dominion KX II:*
1. Using Dominion KX II, create special groups and assign proper permissions and privileges to these groups. For example, create groups such as: KVM_Admin, KVM_Operator.
 2. On your Active Directory server, create new groups with the same group names as in the previous step.
 3. On your AD server, assign the Dominion KX II users to the groups created in step 2.
 4. From the Dominion KX II, enable and configure your AD server properly. Refer to **Implementing LDAP/LDAPS Remote Authentication** (see "Implementing LDAP Remote Authentication" on page 116).

Important Notes:

- Group Name is case sensitive.
- The Dominion KX II provides the following default groups which can not be changed or deleted: Admin and <Unknown>. Please verify that your Active Directory server does not use the same group names.
- If the group information returned from the Active Directory server does not match a Dominion KX II group configuration, the Dominion KX II automatically assigns the group of <Unknown> to users who authenticate successfully.
- If you use a dialback number, you must enter the following case-sensitive string:
msRADIUSCallbackNumber

Implementing RADIUS Remote Authentication

Remote Authentication Dial-in User Service (RADIUS) is an AAA (authentication, authorization, and accounting) protocol for network access applications.

➤ *To use the RADIUS authentication protocol:*

The screenshot shows a configuration window titled "RADIUS". It contains two main sections for "Primary Radius Server" and "Secondary Radius Server". Each section has fields for "Shared Secret", "Authentication Port" (default 1812), "Accounting Port" (default 1813), "Timeout (in seconds)" (default 1), and "Retries" (default 3). At the bottom, there is a "Global Authentication Type" dropdown menu set to "PAP".

1. Type the IP Address of your primary and (optional) secondary remote authentication servers in the Primary Radius Server and Secondary Radius Server fields, respectively.
2. Type the server secret used for authentication (in the Shared Secret fields). The shared secret is a character string that must be known by both the Dominion KX II and the RADIUS server to allow them to communicate securely. It is essentially a password.
3. Authentication Port. The default authentication port is 1812; change as required.

4. Accounting Port. The default accounting port is 1813; change as required.
5. Timeout (in seconds). The default timeout is 1 second; change as required. The timeout is the length of time the Dominion KX II waits for a response from the RADIUS server before sending another authentication request.
6. Retries. The default number of retries is 3; change as required. This is the number of times the Dominion KX II will send an authentication request to the RADIUS server.
7. Global Authentication Type. Choose from among the options in the drop-down list:
 - PAP. With PAP, passwords are sent as plain text. PAP is not interactive; the username and password are sent as one data package once a connection is established, rather than the server sending a login prompt and waiting for a response.
 - CHAP. With CHAP authentication can be requested by the server at any time. CHAP provides more security than PAP.

Returning User Group Information via RADIUS

When a RADIUS authentication attempt succeeds, the Dominion KX II device determines the permissions for a given user based on the permissions of the user's group.

Your remote RADIUS server can provide these user group names by returning an attribute, implemented as a RADIUS FILTER-ID. The FILTER-ID should be formatted as follows:

Raritan:G{GROUP_NAME}

where GROUP_NAME is a string, denoting the name of the group to which the user belongs.

RADIUS Communication Exchange Specifications

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

Attribute	Data
Login	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) for network connections.

Authentication Settings

Attribute	Data
Login	
NAS-IP-Address (4)	The IP Address for the Dominion KX II unit.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
User-Password(2):	The encrypted password.
Accounting-Request(4)	
Acct-Status (40)	Start(1) - Starts the accounting.
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP Address for the Dominion KX II unit.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.
Logout	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - Stops the accounting
NAS-Port-Type (61)	VIRTUAL (5) for network connections.
NAS-Port (5)	Always 0.
NAS-IP-Address (4)	The IP Address for the Dominion KX II unit.
User-Name (1)	The user name entered at the login screen.
Acct-Session-ID (44)	Session ID for accounting.

Chapter 9 Device Management

In This Chapter

Device Management Menu	123
Network Settings	124
Date/Time Settings.....	130
Event Management.....	131
Power Supply Setup Page.....	141
Port Configuration Page	143
Power Control	145

Device Management Menu

The Device Settings menu is organized as follows: Network, Date/Time, Event Management (Settings and Destinations), Power Supply Setup, Port Configuration, and Local Port Settings (Dominion KX II Local Console only).

Use:	To:
Network	Customize the network configuration for the Dominion KX II.
Date/Time	Set date, time, time zone, and Network Time Protocol (NTP).
Event Management - Settings	Configure SNMP and Syslog.
Event Management - Destinations	Select which system events to track and where to send this information.
Power Supply Setup	Configure auto-detection of the Dominion KX II power supplies.
Port Configuration	Configure KVM ports, power CIMs, and outlets.
Local Port Settings	Configure local port; Dominion KX II Local Console only.

Network Settings

Use the Network Settings page to customize the network configuration (e.g., IP Address, discovery port, and LAN interface parameters) for your Dominion KX II unit.

Important: Dominion KX II must be rebooted for new network settings to take effect. Before changing the network configuration, ensure that there are no other active user connections to the device; all connections will be dropped when the Dominion KX II unit reboots.

Basically, there are two ways to setup your IP Configuration:

- None. (Default) This option is the recommended option (Static IP). Since the Dominion KX II is part of your network infrastructure, you most likely do not want its IP Address to change frequently. This option allows you to set the network parameters.
- DHCP. The IP Address is automatically assigned by a DHCP server.

➤ *To change the network configuration:*

1. Choose Device Settings > Network. The Network Settings page opens.

Port Access Virtual Media User Management **Device Settings** Security Maintenance Diagnostics

Home > Device Settings > Network Settings

Network Basic Settings

Device Name *

IP auto configuration

Preferred host name (DHCP only)

IP address

Subnet mask

Gateway IP address

Primary DNS server IP address

Secondary DNS server IP address

Network Miscellaneous Settings

Discovery Port *

Bandwidth Limit

LAN Interface Settings

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

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

LAN Interface Speed & Duplex

☐ Enable Automatic Failover

Ping Interval (seconds) *

Timeout (seconds) *

2. Update the Network Basic Settings. Refer to *Network Basic Settings* (on page 126) for more information about each of the fields.
3. Update the Network Miscellaneous Settings. Refer to *Network Miscellaneous Settings* (on page 127) for more information about each of the fields.
4. Update the LAN Interface Settings. Refer to *LAN Interface Settings* (on page 128) for more information about each of the fields.

Network Settings

- Click OK to set these configurations. If your changes require rebooting the device, a reboot message appears.

➤ *To cancel without saving changes:*

- Click Cancel.

➤ *To reset to factory defaults:*

- Click Reset to Defaults.

Network Basic Settings



The screenshot shows a 'Network Basic Settings' window with the following fields and values:

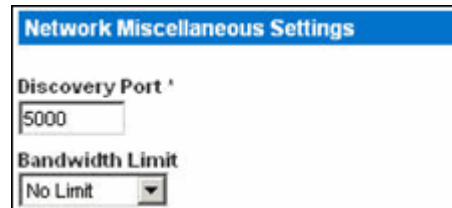
Field	Value
Device Name *	DominionKX
IP auto configuration	None
Preferred host name (DHCP only)	
IP address	192.168.59.97
Subnet mask	255.255.255.0
Gateway IP address	192.168.59.126
Primary DNS server IP address	
Secondary DNS server IP address	

- Device Name. Type a unique name for the device (up to 16 characters; spaces are not allowed). Name your device so you can easily identify it. The default name for a Dominion KX II unit is: "DominionDominion KX II". Remote users will also see this name. However, if an MPC user has created a Connection Profile for this device, that user will see the Description field from the Profile instead.
- IP auto configuration. Select from among the options available in the drop-down list:
 - None. Use this option if you do not want an auto IP configuration and prefer to set the IP Address yourself (static IP). This is the default and recommended option.

If this option is selected for the IP auto configuration, the following Network Basic Settings fields are enabled, allowing you to manually set the IP configuration.

- IP Address. The default IP Address is 192.168.0.192.
- Subnet Mask. The default subnet mask is 255.255.255.0.
- Gateway IP Address. The IP Address for the gateway (if one is used).
- Primary DNS Server IP Address. The primary Domain Name Server used to translate names into IP Addresses.
- Secondary DNS Server IP Address. The secondary Domain Name Server used to translate names into IP Addresses (if one is used).
- DHCP. Dynamic Host Configuration Protocol is used by networked computers (clients) to obtain unique IP addresses and other parameters from a DHCP server.
 - If DHCP is used, enter the Preferred host name (DHCP only). Up to 63 characters.

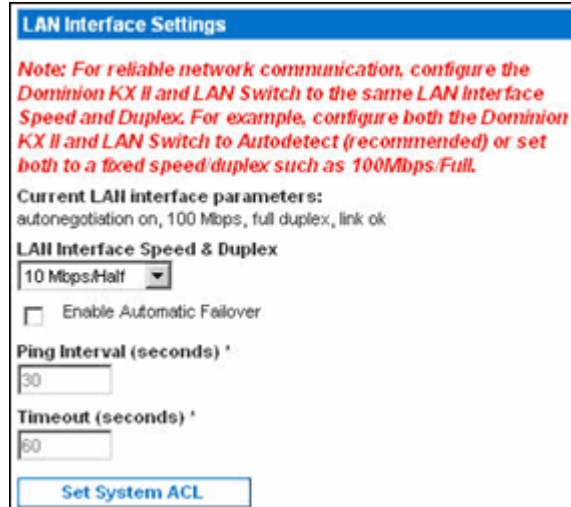
Network Miscellaneous Settings



- Discovery Port. Dominion KX II discovery occurs over a single, configurable TCP Port. The default is Port 5000, but you can configure it to use any TCP port except 80 and 443. To access the Dominion KX II unit from beyond a firewall, your firewall settings must enable two-way communication through the default port 5000 or a non-default port configured here. For more information, refer to *Configure Network Firewall Settings* (see "Change the Keyboard Layout Code (Sun Targets)" on page 29).
- Bandwidth Limit. The default is no limit. Choose from among the options in the drop-down list to set a maximum amount of bandwidth that can be consumed by this Dominion KX II unit (for all sessions). The options include: No Limit, 100 Megabit, 10 Megabit, 5 Megabit, 2 Megabit, 512 Kilobit, 256 Kilobit, and 128 Kilobit.

Note: Lower bandwidth may result in slower performance.

LAN Interface Settings



LAN Interface Settings

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

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

LAN Interface Speed & Duplex
10 Mbps/Half

☐ Enable Automatic Failover

Ping Interval (seconds) *
30

Timeout (seconds) *
60

Set System ACL

- The current parameter settings are identified in the Current LAN interface parameters field.
- LAN Interface Speed & Duplex. Choose from among the speed and duplex combinations available.

Autodetect Default option

10 Mbps/Half

10 Mbps/Full

100 Mbps/Half

100 Mbps/Full

1000 Mbps/Full Gigabit

- Half-duplex provides for communication in both directions, but only one direction at a time (not simultaneously).
- Full-duplex allows communication in both directions simultaneously.

Note: Occasionally there are problems running at 10 Mbps in either half or full duplex. If you are experiencing problems, please try another speed and duplex.

Please refer to *Network Speed Settings* (on page 201) for more information.

- Enable Automatic Failover. Check this checkbox to allow Dominion KX II to automatically recover its network connection using a second network port if the active network port fails. When this option is enabled, the following two fields are used:
 - Ping Interval (seconds). Ping interval determines how often Dominion KX II checks the status of the network connection (setting this too low may cause excess network traffic). The default Ping Interval is 30 seconds.
 - Timeout (seconds). Timeout determines how long a network port must be “dead” before the switch is made. Both network ports must be connected to the network and this option must be checked for Automatic Failover to function. The default Timeout is 60 seconds.

Note: The default Ping Interval and Timeout generate a condition that when the KX device tries to switch over, remote sessions will be dropped and must be re-established. Reducing these intervals to much lower values will allow remote sessions to stay connected, but will result in increased network traffic.

- Set System ACL. Click this button to set a global-level Access Control List for your Dominion KX II by ensuring that your device does not respond to packets being sent from disallowed IP addresses. The *IP Access Control* (on page 160) page opens.

*Note: These ACL values are global, affecting the Dominion KX II unit as a whole. You can also create ACLs on a group-level basis. For example, you can create an “Outsourced Vendors” user group that is permitted to access Dominion KX II only from a given IP address range (refer to **Group-based IP ACL** (see “Group-based IP ACL (Access Control List)” on page 110) for more information on how to create group-specific Access Control Lists).*

Date/Time Settings

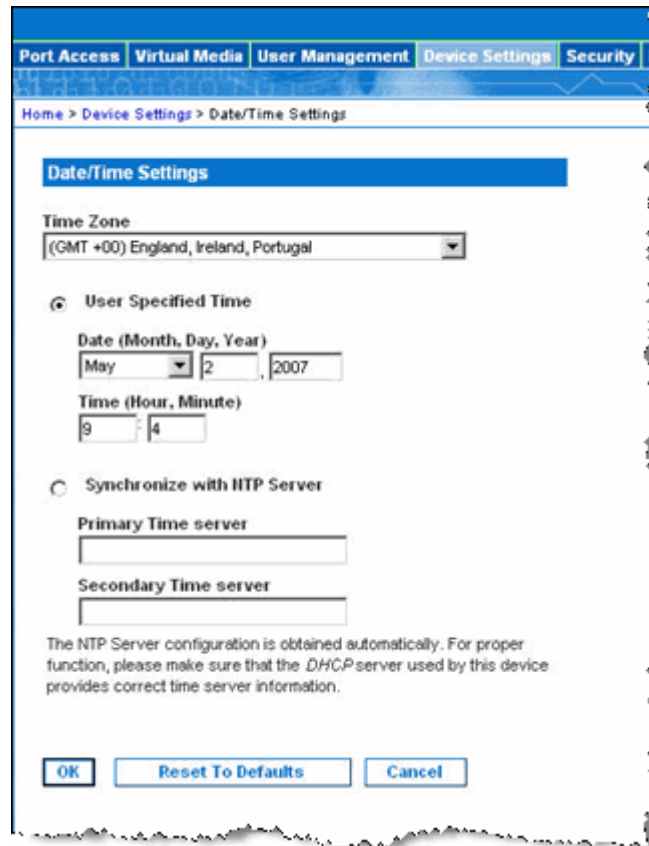
Use the Date/Time Settings page to specify the date and time for the Dominion KX II. There are two ways to do this:

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

Note: The Dominion KX II does not support Daylight Savings Time.

➤ *To set the date and time:*

1. Choose Device Settings > Date/Time. The Date/Time Settings page opens:



The screenshot shows the 'Date/Time Settings' page within a web interface. At the top, there is a navigation bar with tabs: 'Port Access', 'Virtual Media', 'User Management', 'Device Settings' (which is active), and 'Security'. Below the navigation bar, a breadcrumb trail reads 'Home > Device Settings > Date/Time Settings'. The main content area is titled 'Date/Time Settings' and contains the following elements:

- A 'Time Zone' dropdown menu currently set to '(GMT +00) England, Ireland, Portugal'.
- Two radio buttons for selecting the time setting method:
 - ☒ 'User Specified Time': This option is selected. It includes a 'Date (Month, Day, Year)' section with a month dropdown (set to 'May'), a day input (set to '2'), and a year input (set to '2007'). Below this is a 'Time (Hour, Minute)' section with an hour input (set to '9') and a minute input (set to '4').
 - ☐ 'Synchronize with NTP Server': This option is unselected. It includes two text input fields for 'Primary Time server' and 'Secondary Time server'.
- A note at the bottom: 'The NTP Server configuration is obtained automatically. For proper function, please make sure that the DHCP server used by this device provides correct time server information.'
- Three buttons at the bottom: 'OK', 'Reset To Defaults', and 'Cancel'.

2. Choose your time zone from the Time Zone drop-down list.
3. Choose the method you would like to use to set the date and time:
 - User Specified Time. Choose this option to input the date and time manually.

- Synchronize with NTP Server. Choose this option to synchronize the date and time with the Network Time Protocol (NTP) Server.
4. For the User Specified Time option, enter the date and time as follows:
 - a. Choose the Month from the drop-down list.
 - b. Type the Day of the Month.
 - c. Type the Year in yyyy format.
 - d. Type the Time in hh:mm format (using a 24-hour clock).
 5. For the Synchronize with NTP Server option:
 - a. Enter the IP address of the Primary Time server.
 - b. (Optional) Enter the IP address of the Secondary Time server.
 6. Click OK.

Event Management

The Dominion KX II Event Management feature provides a set of screens for enabling and disabling the distribution of system events to SNMP Managers, Syslog, and the audit log. These events are categorized, and for each event you can determine whether you want the event sent to one or several destinations.

Event Management - Settings

SNMP Configuration

Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions. Dominion KX II offers SNMP Agent support through Event Management. Refer to *SNMP Agent Configuration* (on page 138) and *SNMP Trap Configuration* (on page 138) for more information about SNMP Agents and Traps.

➤ *To configure SNMP (enable SNMP logging):*

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

The screenshot shows the 'Event Management - Settings' page. At the top, there is a navigation bar with tabs: Port Access, Virtual Media, User Management, Device Settings (selected), Security, and Maintenance. Below the navigation bar is a breadcrumb trail: Home > Device Settings > Event Management - Settings.

The main content area is divided into two sections:

SNMP Configuration

- ☐ SNMP Logging Enabled
- Name:
- Contact:
- Location:
- Agent Community String:
- Type:

Destination IP	Port #	Community
<input type="text"/>	162	<input type="text"/>
<input type="text"/>	162	<input type="text"/>
<input type="text"/>	162	<input type="text"/>
<input type="text"/>	162	<input type="text"/>
<input type="text"/>	162	<input type="text"/>

[Click here to view the Dominion-KX2 SNMP MB](#)

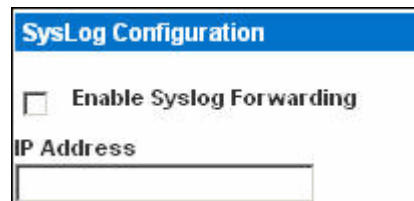
Syslog Configuration

- ☐ Enable Syslog Forwarding
- IP Address:

At the bottom of the page are three buttons: OK, Reset To Defaults, and Cancel.

2. Choose the Enable SNMP Logging option; this enables the remaining SNMP fields.
3. In the Name, Contact, and Location fields, type the SNMP Agent's (this Dominion unit's) name as it appears in the Dominion KX II Console interface, a contact name related to this unit, and where the Dominion unit is physically located, respectively.
4. Type the Agent Community String (the Dominion unit's string). An SNMP community is the group that devices and management stations running SNMP belong to; it helps define where information is sent. The community name is used to identify the group; an SNMP device or agent may belong to more than one SNMP community.
5. Specify whether the community is Read-Only or Read-Write using the Type drop-down list.
6. Configure up to five SNMP managers by specifying their Destination IP, Port #, and Community.
7. Click the Click here to view the Dominion- SNMP MIB link to access the SNMP Management Information Base.
8. Click OK.

Syslog Configuration



➤ *To configure the Syslog (enable Syslog forwarding):*

1. Choose the Enable Syslog Forwarding option to log the device's messages to a remote Syslog server.
2. Type the IP Address of your Syslog server in the IP Address field.
3. Click OK.

Event Management

➤ *To cancel without saving changes:*

- Click Cancel.

➤ *To reset to factory defaults:*

- Click the Reset To Defaults button.

SNMP Configuration

Simple Network Management Protocol (SNMP) is a protocol governing network management and the monitoring of network devices and their functions. Dominion KX II offers SNMP Agent support through Event Management. Refer to *SNMP Agent Configuration* (on page 138) and *SNMP Trap Configuration* (on page 138) for more information about SNMP Agents and Traps.

➤ *To configure SNMP (enable SNMP logging):*

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

Port Access Virtual Media User Management **Device Settings** Security Maintenance

Home > Device Settings > Event Management - Settings

SNMP Configuration

☐ SNMP Logging Enabled

Name
DominionOX

Contact

Location

Agent Community String

Type
Read-Only

Destination IP	Port #	Community
	162	
	162	
	162	
	162	
	162	

[Click here to view the Dominion-KX2 SNMP MB](#)

Syslog Configuration

☐ Enable Syslog Forwarding

IP Address

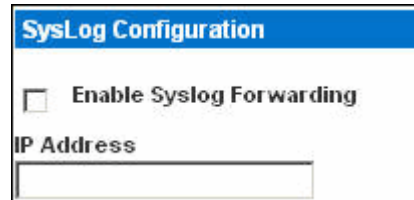
OK Reset To Defaults Cancel

2. Choose the Enable SNMP Logging option; this enables the remaining SNMP fields.
3. In the Name, Contact, and Location fields, type the SNMP Agent's (this Dominion unit's) name as it appears in the Dominion KX II Console interface, a contact name related to this unit, and where the Dominion unit is physically located, respectively.
4. Type the Agent Community String (the Dominion unit's string). An SNMP community is the group that devices and management stations running SNMP belong to; it helps define where information is sent. The community name is used to identify the group; an SNMP device or agent may belong to more than one SNMP community.
5. Specify whether the community is Read-Only or Read-Write using the Type drop-down list.
6. Configure up to five SNMP managers by specifying their Destination IP, Port #, and Community.

Event Management

7. Click the Click here to view the Dominion- SNMP MIB link to access the SNMP Management Information Base.
8. Click OK.

Syslog Configuration

A screenshot of a web-based configuration dialog box titled "SysLog Configuration". The dialog has a blue header bar with the title. Below the header, there is a checkbox labeled "Enable Syslog Forwarding". Underneath the checkbox is a text input field labeled "IP Address". The input field is currently empty.

- *To configure the Syslog (enable Syslog forwarding):*
 1. Choose the Enable Syslog Forwarding option to log the device's messages to a remote Syslog server.
 2. Type the IP Address of your Syslog server in the IP Address field.
 3. Click OK.
- *To cancel without saving changes:*
 - Click Cancel.
- *To reset to factory defaults:*
 - Click the Reset To Defaults button.

Event Management - Destinations

System events, if enabled, can generate SNMP notification events (traps), or can be logged to Syslog or Audit Log. Use the Event Management - Destinations page to select which system events to track and where to send this information.

Note: SNMP traps will only be generated if the SNMP Logging Enabled option is checked; Syslog events will only be generated if the Enable Syslog Forwarding option is checked. Both of these options are in the Event Management - Settings page.

➤ To select events and their destinations:

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

Category	Event	SNMP	Syslog	Audit Log
Device Operation	System Startup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Power Supply Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Powerstrip Outlet Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Parameter Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Ethernet Failover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Management	Factory/Reset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Begin OC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	End OC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Started	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Completed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware Update Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware File Discarded	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware Validation Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Configuration Backed Up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security	Configuration Restored	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Connection Denied	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Password Settings Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Login Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Activity	Password Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User Blocked	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Connected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Disconnected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

System events are categorized by Device Operation, Device Management, Security, User Activity, and User Group Administration.

2. Select the checkboxes for those Event line items you want to enable or disable, and where you want to send the information.

Tip: Enable or disable entire Categories by checking or clearing the Category line checkboxes, respectively.

3. Click OK.

➤ *To cancel without saving changes:*

- Click Cancel.

➤ *To reset to factory defaults:*

- Click the Reset To Defaults button.

SNMP Agent Configuration

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

SNMP Trap Configuration

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

Trap Name	Description
configBackup	The device configuration has been backed up.
configRestore	The device configuration has been restored.
deviceUpdateFailed	Device update has failed.
deviceUpgradeCompleted	The Dominion KX II has completed update via an RFP file.
deviceUpgradeStarted	The Dominion KX II has begun update via an RFP file.
factoryReset	The device has been reset to factory defaults.
firmwareFileDiscarded	Firmware file was discarded.
firmwareUpdateFailed	Firmware update failed.
firmwareValidationFailed	Firmware validation failed.

Trap Name	Description
groupAdded	A group has been added to the Dominion KX II system.
groupDeleted	A group has been deleted from the system.
groupModified	A group has been modified.
ipConflictDetected	An IP Address conflict was detected.
ipConflictResolved	An IP Address conflict was resolved.
networkFailure	An Ethernet interface of the product can no longer communicate over the network.
networkParameterChanged	A change has been made to the network parameters.
passwordSettingsChanged	Strong password settings have changed.
portConnect	A previously authenticated user has begun a KVM session.
portConnectionDenied	A connection to the target port was denied.
portDisconnect	A user engaging in a KVM session closes the session properly.
portStatusChange	The port has become unavailable.
powerNotification	The power outlet status notification: 1=Active, 0=Inactive.
powerOutletNotification	Power strip device outlet status notification.
rebootCompleted	The Dominion KX II has completed its reboot.
rebootStarted	The Dominion KX II has begun to reboot, either through cycling power to the system or by a warm reboot from the OS.
securityViolation	Security violation.
startCCManagement	The device has been put under CommandCenter Management.
stopCCManagement	The device has been removed from CommandCenter Management.
userAdded	A user has been added to the system.
userAuthenticationFailure	A user attempted to log in without a correct username and/or password.

Event Management

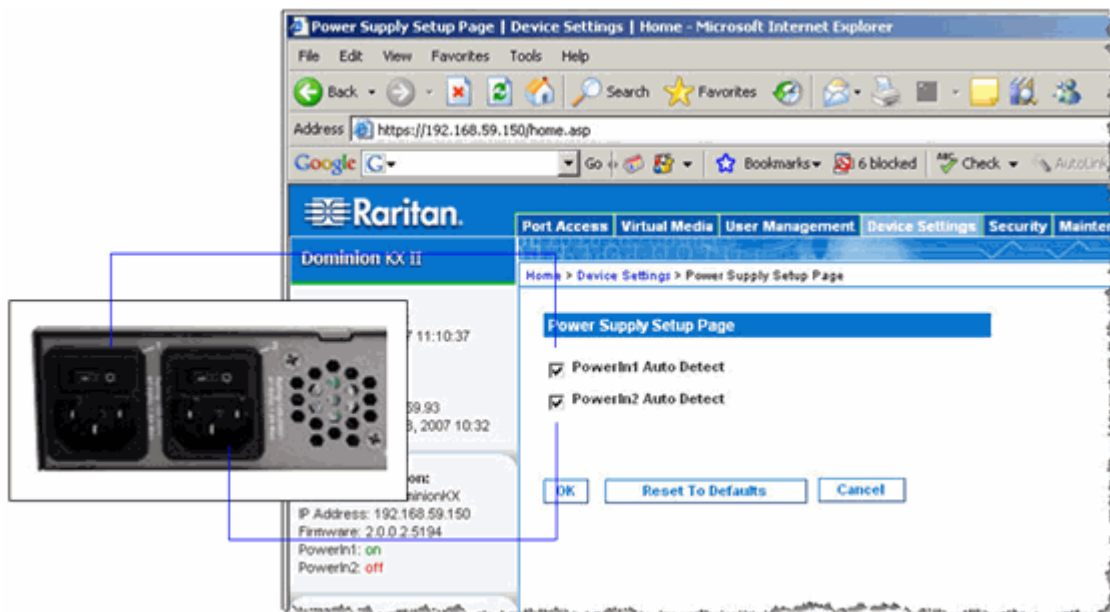
Trap Name	Description
userConnectionLost	A user with an active session has experienced an abnormal session termination.
userDeleted	A user account has been deleted.
userLogin	A user has successfully logged into the Dominion KX II and has been authenticated.
userLogout	A user has successfully logged out of the Dominion KX II properly.
userModified	A user account has been modified.
userPasswordChanged	This event is triggered if the password of any user of the device is modified.
userSessionTimeout	A user with an active session has experienced a session termination due to timeout.
vmImageConnected	User attempted to mount either a device or image on the target using Virtual Media. For every attempt on device/image mapping (mounting) this event is generated.
vmImageDisconnected	User attempted to unmount a device or image on the target using Virtual Media.

Power Supply Setup Page

The Dominion KX II provides dual power supplies, and can automatically detect and provide notification regarding the status of these power supplies. Use the Power Supply Setup page to specify whether you are using one or both of the power supplies. Proper configuration ensures that the Dominion KX II sends the appropriate notifications should a power supply fail. For example, if power supply number one fails, the power LED at the front of the unit will turn red.

➤ *To enable automatic detection for the power supplies in use:*

1. Choose Device Settings > Power Supply Setup. The Power Supply Setup page opens:



2. If you are plugging power input into power supply number one (left-most power supply at the back of the unit), then select the PowerIn1 Auto Detect option.
3. If you are plugging power input into power supply number two (right-most power supply at the back of the unit), then select the PowerIn2 Auto Detect option.
4. Click OK.

Note: If either of these checkboxes is selected and power input is not actually connected, the power LED at the front of the unit displays red.

➤ *To turn off the automatic detection:*

Deselect the checkbox for the appropriate power supply.

➤ *To reset to factory defaults:*

- Click the Reset To Defaults button.

➤ *To cancel without saving changes:*

- Click the Cancel button.

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

Port Configuration Page

The Port Configuration page displays a list of the Dominion KX II ports. Ports connected to KVM target servers or power strips are displayed in blue and can be edited. For ports with no CIM connected or with a blank CIM name, a default port name of Dominion-KX2_Port# is assigned, where Port# is the number of the Dominion KX II physical port.

➤ *To change a port configuration:*

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

Port Number	Port Name	Port Type
1	Dominion-KX2_Port1	Not Available
2	Dominion-KX2_Port2	Not Available
3	Dominion-KX2_Port3	Not Available
4	Dominion-KX2_Port4	Not Available
5	JLtestPC	DCIM
6	Dominion-KX2_Port6	Not Available
7	Dominion-KX2_Port7	Not Available
8	Dominion-KX2_Port8	Not Available
9	Local Port	VM
10	Dominion-KX2_Port10	Not Available
11	Dominion-KX2_Port11	Not Available
12	Dominion-KX2_Port12	Not Available
13	Dominion-KX2_Port13	Not Available
14	Dominion-KX2_Port14	Not Available
15	Dominion-KX2_Port15	Not Available
16	PowerStrip	PowerStrip

Copyright © 2007 Raritan Computer Inc.

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

- Port Number. Numbered from 1 to the total number of ports available for the Dominion KX II unit.
- Port Name. The name assigned to the port. A port name displayed in black indicates that you cannot change the name and that the port cannot be edited; port names displayed in blue can be edited.

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

- Port Type. The type of CIM connected to the port:

Port Type	Description
DCIM	Dominion CIM
Not Available	No CIM connected
PCIM	Paragon CIM
PowerStrip	Power CIM
VM	Virtual Media CIM (D2CIM-VUSB)

2. Click the Port Name for the port you want to edit.
 - For KVM ports, the **Port page** (see "Associate KVM Target Servers to Outlets (Port Page)" on page 149) is opened. From this page, you can name the ports and create power associations.
 - For power strips, the Port page for **power strips** (see "Name the Power Strip (Port Page for Power Strips)" on page 147) is opened. From this page, you can name the power strips and their outlets. name the power strips and their outlets.

Chapter 10

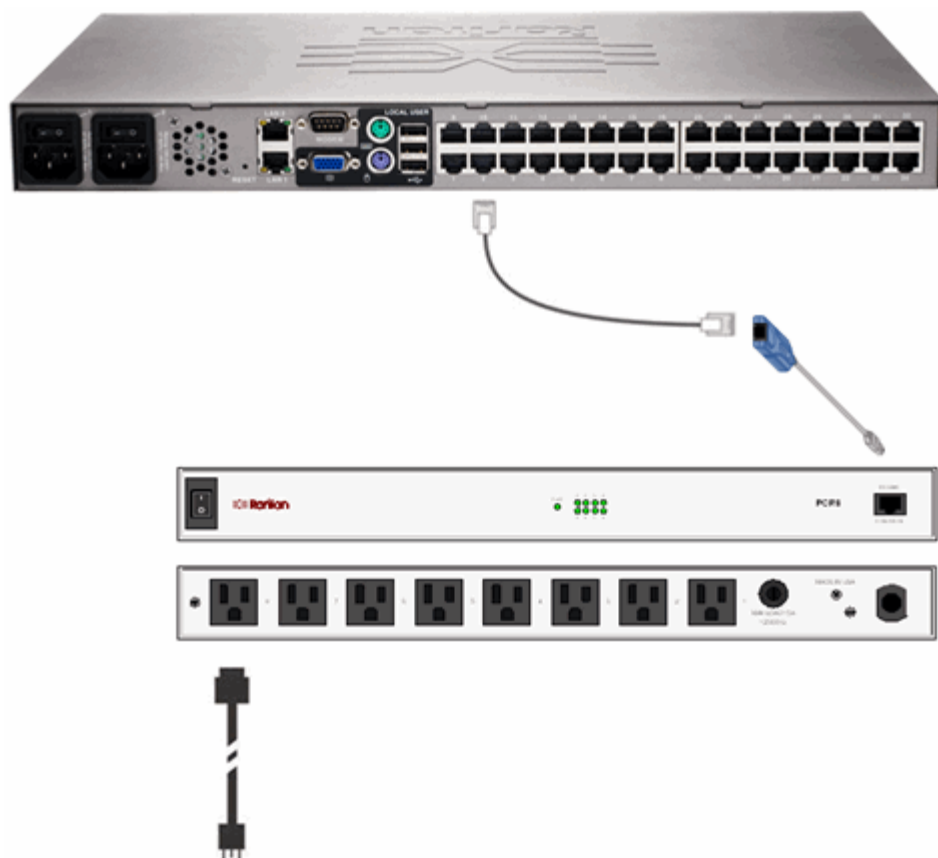
Power Control

In This Chapter

Connect the Power Strip	145
Name the Power Strip (Port Page for Power Strips)	147
Associate KVM Target Servers to Outlets (Port Page)	149
Note for D2CIM-VUSB CIM Usage (Shared)	151

Connect the Power Strip

The numbers in this diagram correspond to the steps listed below.



➤ *To connect the power strip:*

1. Connect the male RJ-45 of the D2CIM-PWR to the female RJ-45 connector on the power strip.

Power Control

2. Connect the female RJ-45 connector of the D2CIM-PWR to any of the available female system port connectors on the Dominion KX II using a straight through Cat 5 cable.
3. Attach an AC power cord to the target server and an available power strip outlet.
4. Connect the power strip to an AC power source.
5. Power ON the Dominion KX II unit.

Name the Power Strip (Port Page for Power Strips)

This Port page opens when you select a port from the *Port Configuration* (see "Port Configuration Page" on page 143) page that is connected to a Raritan remote power strip. The Type and the Name fields are pre-populated; please note that the (CIM) Type cannot be changed. The following information is displayed for each outlet in the power strip: outlet Number, Name, and Port Association.

Use this page to name the power strip and its outlets; all names can be up to 32 alphanumeric characters and can include *special characters* (see "Valid Special Characters" on page 33).

The screenshot shows the 'Port' configuration page for a Power Strip. The 'Port' section has a 'Type' of 'PowerStrip' and a 'Name' of 'PCR8'. Below this is the 'Outlets' section, which is a table with 8 rows. Each row has a 'Number' (1-8), a 'Name' field, and a 'Port Association' field. The 'Port Association' for all outlets is 'TestPC'. At the bottom of the page are 'OK' and 'Cancel' buttons.

Number	Name	Port Association
1	TestPC(1)	TestPC
2	Outlet 2	
3	Outlet 3	
4	Outlet 4	
5	Outlet 5	
6	Outlet 6	
7	Outlet 7	
8	Outlet 8	

Power Control

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

➤ *To name the power strip (and outlets):*

Note: CommandCenter Service Gateway does not recognize power strip names containing spaces.

1. Change the Name of the power strip to something you will remember.
2. Change the (Outlet) Name if desired. (Outlet names default to Outlet #.)
3. Click OK.

➤ *To cancel without saving changes:*

- Click Cancel.

Associate KVM Target Servers to Outlets (Port Page)

This Port page opens when you select a port from the *Port Configuration* (see "Port Configuration Page" on page 143) page that is connected to a target server. From this page, you can make power associations, change the Port Name to something more descriptive, and update target server settings if you are using the *D2CIM-VUSB CIM* (see "Note for D2CIM-VUSB CIM Usage (Shared)" on page 151). The (CIM) Type and the (Port) Name fields are pre-populated; please note that the CIM type cannot be changed.

A server can have up to four power plugs and you can associate a different power strip with each. From this page, you can define those associations so that you can power on, power off, and power cycle the server from the Port Access page.

To use this feature, you will need:

- Raritan remote power strip(s)
- Power CIMs (D2CIM-PWR)

The screenshot shows the Raritan web interface for Port Configuration. The breadcrumb trail is: Home > Device Settings > Port Configuration > Port. The page has a blue header with tabs: Port Access, Virtual Media, User Management, Device Settings, Security, and Maintenance. The main content area is titled "Port" and contains the following fields:

- Type:** PCM
- Name:** Dominion-KX2_Port5

Below the Port section is the "Power Association" section, which contains two columns of dropdown menus:

Power Strip Name	Outlet Name
Domination-KX2_Port16	Outlet 8
Domination-KX2_Port16	None
None	---
None	---

At the bottom of the form are "OK" and "Cancel" buttons.

- *To make power associations (associate power strip outlets to KVM target servers):*

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

1. Choose the power strip from the Power Strip Name drop-down list.
2. For that power strip, choose the outlet from the Outlet Name drop-down list.
3. Repeat steps 1 and 2 for all desired power associations.
4. Click OK. A confirmation message is displayed.

- *To change the port name:*

1. Type something descriptive in the Name field. For example, the name of the target server would be a likely candidate. The name can be up to 32 alphanumeric characters and can include *special characters* (see "Valid Special Characters" on page 33).
2. Click OK.

- *To cancel without saving changes:*

- Click Cancel.

- *To remove a power strip association:*

1. Select the appropriate power strip from the Power Strip Name drop-down list.
2. For that power strip, select the appropriate outlet from the Outlet Name drop-down list.
3. From the Outlet Name drop-down list, select None.
4. Click OK. That power strip/outlet association is removed. A confirmation message is displayed.

Note for D2CIM-VUSB CIM Usage (Shared)

If you are using the D2CIM-VUSB, there are additional settings on the Port page to improve performance.

Port Access Virtual Media User Management **Device Settings** Security

Home > Device Settings > Port Configuration > Port

Port

Type:
VM

Name:
Dominion-KX2_Port3

Power Association

Power Strip Name	Outlet Name
None	---
None	---
None	---
None	---

Target Server Settings

☐ Absolute mouse scaling for MAC server

☐ Use Full Speed for Virtual Media CIM - Useful for BIOS that cannot handle High Speed USB devices

OK Cancel

If you are experiencing synchronization issues and are using the D2CIM-VUSB CIM for a Mac target server, check the Absolute mouse scaling for MAC server option.

Certain BIOS do not support USB high-speed capabilities and the attempt to auto-negotiate does not work. If you are experiencing BIOS problems with the target server, check the Use Full Speed for Virtual Media CIM option.

Note: For SUSE 9.2 KVM target servers, please enable (check) the Use Full Speed for Virtual Media CIM option for those target server ports. SUSE 9.2 does not work with the Virtual Media CIM when high speed is negotiated.

Chapter 11 Security Settings

In This Chapter

Security Settings Menu	152
Security Settings.....	153
IP Access Control.....	160

Security Settings Menu

The Security menu is organized as follows: Security Settings and IP Access Control.

Use:	To:
Security Settings	Configure security settings for login limitations, strong passwords, user blocking, and encryption & share.
IP Access Control	Control access to your Dominion KX II unit. By setting a global access control list, you are by ensuring that your device does not respond to packets being sent from disallowed IP addresses.

Security Settings

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

Raritan SSL certificates are used for public and private key exchanges, and provide an additional level of security. Raritan web server certificates are self-signed; Java applet certificates are signed by a VeriSign certificate. Encryption guarantees that your information is safe from eavesdropping and these certificates ensure that you can trust that the entity is Raritan, Inc.

➤ *To configure the security settings:*

1. Choose Security > Security Settings. The Security Settings page opens.

The fields are organized into the following groups: Login Limitations, Strong Passwords, User Blocking, and Encryption & Share.

2. Update the *Login Limitations* (on page 154) settings as appropriate.
3. Update the *Strong Passwords* (on page 155) settings as appropriate.
4. Update the *User Blocking* (on page 156) settings as appropriate.

Security Settings

5. Update the *Encryption & Share* (on page 157) settings as appropriate.
 6. Click OK.
- *To close the page without saving any changes:*
- Click Cancel.
- *To reset back to defaults:*
- Click Reset to Defaults.

Login Limitations

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

- Enable Single Login Limitation. When selected only one login per username is allowed at any time. When deselected, a given username/password combination can be connected into the device from several client workstations simultaneously.
- Enable Password Aging. When selected all users are required to change their passwords periodically, based on the number of days specified in Password Aging Interval field.
 - Password Aging Interval (days). This field is enabled and required when the Enable Password Aging checkbox is selected. Enter the number of days after which a password change is required. The default is 60 days.
- Log Out Idle Users. Select the checkbox to automatically disconnect a user session after a certain amount of inactive time has passed. Type the amount of time in the After field. If there is no activity from the keyboard or mouse, all sessions and all resources are logged out. If a Virtual Media session is in progress, however, the session does not timeout.
 - After (minutes). The amount of time (in minutes) after which an idle user will be logged out. This field is enabled when the Log Out Idle Users option is selected.

Strong Passwords

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

- Enable strong passwords. Strong passwords require user-created passwords to have a minimum of 8 characters with at least one alphabetical character and one non-alphabetical character (punctuation character or number). In addition, the first four characters of the password and the username cannot match. When selected, strong password rules are enforced. Users with passwords not meeting strong password criteria will automatically be required to change their password on their next login. When deselected, only the standard format validation is enforced. When selected, the following fields are enabled and required:
 - Minimum length of strong password. Passwords must be at least 8 characters long. The default is 8, but it can be up to 63.
 - Maximum length of strong password. The default is 16, but can be up to 64 characters long.
 - Enforce at least one lower case character. When checked, at least one lower case character is required in the password.
 - Enforce at least one upper case character. When checked, at least one upper case character is required in the password.
 - Enforce at least one numeric character. When checked, at least one numeric character is required in the password.

Security Settings

- Enforce at least one printable special character. When checked, at least one special character (printable) is required in the password.
- Number of restricted passwords based on history. This field represents the password history depth; that is, the number of prior passwords that cannot be repeated. The range is 1-12; the default is 5.

User Blocking

The User Blocking options specify the criteria by which users are blocked from accessing the system after the specified number of unsuccessful login attempts. The three options are mutually exclusive:

- Disabled. The default option; users are not blocked regardless of the number of times they fail authentication.
- Timer Lockout. Users are denied access to the system for the specified amount of time after exceeding the specified number of unsuccessful login attempts. When selected, the following fields are enabled:
 - Attempts. The number of unsuccessful login attempts after which the user will be locked out. The valid range is 1 - 10; the default is 3 attempts.
 - Lockout Time. The amount of time for which the user will be locked out. The valid range is 1 - 1440 minutes; the default is 5 minutes.

- Deactivate User-ID. When selected, this option specifies that the user will be locked out of the system after the number of failed login attempts specified in the Failed Attempts field:
 - Failed Attempts. The number of unsuccessful login attempts after which the user's User-ID will be deactivated. This field is enabled when the Deactivate User-ID option is selected. The valid range is 1 - 10.

The screenshot shows a window titled "User Blocking". It contains three radio button options: "Disabled", "Timer Lockout", and "Deactivate User-ID". The "Deactivate User-ID" option is selected. Below the radio buttons, there are two input fields: "Attempts" and "Failed Attempts". Both fields have the value "3" entered. There is also a "Lockout Time" field with the value "5" entered.

When a user-ID is deactivated after the specified number of failed attempts, the administrator must change the user password and activate the user account by selecting the Active checkbox on the *User* (see "Add New User" on page 102) page.

Encryption & Share

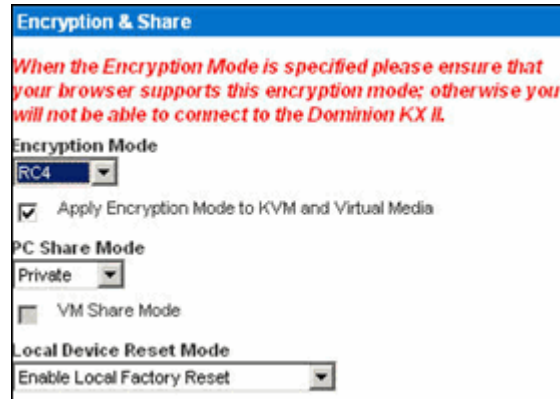
Using the Encryption & Share settings you can specify the type of encryption used, PC and VM share modes, and the type of reset performed when the Dominion KX II reset button is pressed.

The screenshot shows a window titled "Encryption & Share". It contains several settings:

- Encryption Mode:** A dropdown menu set to "Auto".
- Apply Encryption Mode to KVM and Virtual Media:** A checked checkbox.
- PC Share Mode:** A dropdown menu set to "Private".
- VM Share Mode:** An unchecked checkbox.
- Local Device Reset Mode:** A dropdown menu set to "Enable Local Factory Reset".

Security Settings

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



- Auto. This is the recommended option; the Dominion KX II auto-negotiates to the highest level of encryption possible.
 - RC4. Secures user names, passwords and KVM data, including video transmissions using the RSA RC4 encryption method. This is a 128-bit Secure Sockets Layer (SSL) protocol which provides a private communications channel between the Dominion KX II unit and the Remote PC during initial connection authentication.
 - AES-128. The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology specification for the encryption of electronic data; 128 is the key length. When AES-128 is specified, please be certain that your browser supports it, otherwise you will not be able to connect. Please refer to *Checking Your Browser for AES Encryption* (on page 160) for more information.
- Apply Encryption Mode to KVM and Virtual Media. When selected, this option applies the selected encryption mode to both KVM and virtual media. After authentication, KVM and virtual media data is also transferred with 128-bit encryption.
 - PC Share Mode. Determines global concurrent remote KVM access, enabling up to eight remote users to simultaneously log on to one Dominion KX II and concurrently view and control the same target server through the device. Click on the drop-down list to select one of the following options:
 - Private: No PC share; this is the default mode. Each target server can be accessed exclusively by only one user at a time.

- PC-Share: KVM target servers can be accessed by up to eight users (administrator or non-administrator) at one time. Each remote user has equal keyboard and mouse control, however, please note that uneven control will occur if one user does not stop typing or moving the mouse.
- VM Share Mode. This option is enabled only when PC-Share Mode is enabled. When selected, this option permits the sharing of virtual media among multiple users, that is, several users can access the same virtual media session. The default is disabled.
- Local Device Reset Mode. This option specifies which actions are taken when the hardware reset button (at the back of the unit) is depressed. For more information, refer to **Reset Button** (on page 184). Choose one of the following options:
 - Enable Local Factory Reset (Default). Returns the Dominion KX II unit to the factory defaults.
 - Enable Local Admin Password Reset. Resets the local administrator password only. The password is reset to raritan.
 - Disable All Local Resets. No reset action is taken.

Checking Your Browser for AES Encryption

If you do not know if your browser uses AES, check with the browser manufacturer, or navigate to the following website using the browser with the encryption method you want to check:

<https://www.fortify.net/sslcheck.html>. This website detects your browser's encryption method and displays a report.

Note: IE6 does not support AES 128 or 256-bit encryption.

AES 256 Prerequisites and Supported Configurations

AES 256-bit encryption is supported on the following web browsers only:

- Firefox 2.0.0.7
- Mozilla 1.7.13
- Internet Explorer 7

In addition to browser support, AES 256-bit encryption requires the installation of Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

Jurisdiction files for various JRE's are available at the "other downloads" section of the following links:

- JRE1.4.2 - <http://java.sun.com/j2se/1.4.2/download.html>
- JRE1.5 - http://java.sun.com/javase/downloads/index_jdk5.jsp

IP Access Control

Using IP Access Control, you can control access to your Dominion KX II unit. By setting a global Access Control List (ACL) you are by ensuring that your device does not respond to packets being sent from disallowed IP addresses. The IP Access Control is global, affecting the Dominion KX II unit as a whole, but you can also control access to your unit at the group level. Refer to *group-based IP Access Control* (see "Group-based IP ACL (Access Control List)" on page 110) for more information about group-level control.

Important: IP Address 127.0.0.1 is used by the Dominion KX II local port. When creating an IP Access Control list, if 127.0.0.1 is within the range of IP Addresses that are blocked, you will not have access to the Dominion KX II local port.

➤ *To use IP Access Control:*

1. Open the IP Access Control page using one of these methods:
 - Choose Security > IP Access Control, or
 - Click the Set System ACL button from the *Network Settings* (on page 124) page

The IP Access Control page opens:

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

➤ *To add (append) rules:*

1. Type the IP Address and subnet mask in the IP/Mask field.
2. Choose the Policy from the drop-down list.
3. Click Append. The rule is added to the bottom of the rules list.
4. Repeat steps 1 through 3 for each rule you want to enter.

➤ *To insert a rule:*

1. Type a Rule #. A Rule # is required when using the Insert command.
2. Type the IP Address and subnet mask in the IP/Mask field.
3. Choose the Policy from the drop-down list.
4. Click Insert. If the Rule # you just typed equals an existing Rule #, the new rule is placed ahead of the exiting rule and all rules are moved down in the list.

➤ *To replace a rule:*

1. Specify the Rule # you want to replace.
2. Type the IP Address and subnet mask in the IP/Mask field.
3. Choose the Policy from the drop-down list.
4. Click Replace. Your new rule replaces the original rule with the same Rule #.

➤ *To delete a rule:*

1. Specify the Rule # you want to delete.
2. Click Delete.
3. You are prompted to confirm the deletion. Click OK.

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

Chapter 12 Maintenance

In This Chapter

Maintenance Menu	163
Maintenance Features (Local/Remote Console)	163
Audit Log.....	164
Device Information.....	166
Backup and Restore	167
CIM Upgrade.....	169
Upgrade History	171
Reboot.....	172

Maintenance Menu

The Maintenance menu includes these options:

- Audit Log
- Device Information
- Backup/Restore
- CIM Firmware Upgrade
- Firmware Upgrade
- Factory Reset (Dominion KX II Local Console only)
- Reboot
- Upgrade History

Maintenance Features (Local/Remote Console)

Use:	To:	Local	Remote
Audit Log	View Dominion Dominion KX II events sorted by date and time.	✓	✓
Device Information	View information about the Dominion Dominion KX II and its CIMs.	✓	✓
Backup/Restore	Backup and restore the Dominion KX II configuration.		✓

Audit Log

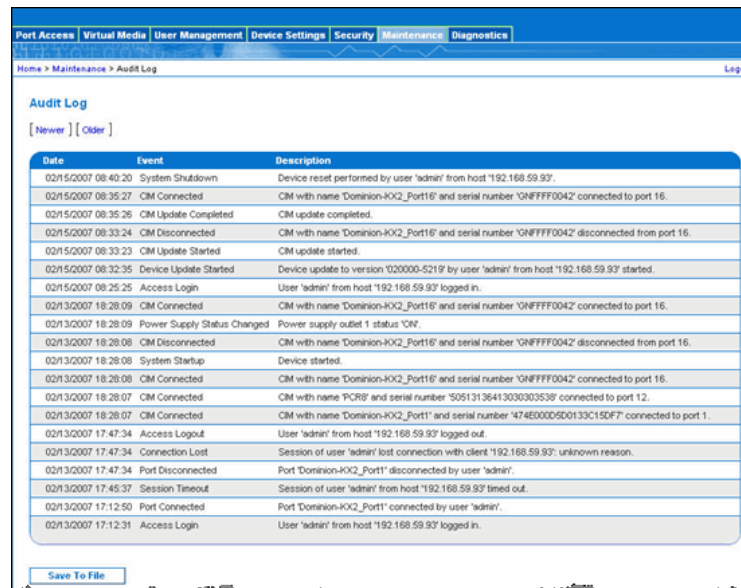
Use:	To:	Local	Remote
CIM Firmware Upgrade	Upgrade your CIMs using the firmware versions stored in the Dominion Dominion KX II memory.	✓	✓
Firmware Upgrade	Upgrade your Dominion Dominion KX II firmware.		✓
Factory Reset	Perform a factory reset.	✓	
Upgrade History	View information about the latest upgrade performed.	✓	✓
Reboot	Reboot the Dominion Dominion KX II unit.	✓	✓

Audit Log

A log is created of Dominion KX II system events.

➤ To view the audit log for your Dominion KX II unit:

1. Choose Maintenance > Audit Log. The Audit Log page opens:



The Audit Log page displays events by date and time (most recent events listed first). The Audit Log provides the following information:

- Date. The date and time that the event occurred; 24-hour clock.
- Event. The event name as listed in the Event Management page.
- Description. Detailed description of the event.

➤ *To save the Audit Log:*

Note: Saving the Audit Log is available only on the Dominion KX II Remote Console, not on the Local Console.

1. Click the Save to File button. A Save File dialog box opens.
2. Choose the desired file name and location and click Save. The audit log is saved locally on your client machine with the name and location specified.

➤ *To page through the Audit Log:*

- Use the [Older] and [Newer] links.

Device Information

The Device Information page provides detailed information about your Dominion KX II device and the CIMs in use. This information is helpful should you need to contact Raritan Technical Support.

- To view information about your Dominion KX II and CIMs:
 - Choose Maintenance > Device Information. The Device Information page opens:

The screenshot shows the 'Device Information' page. At the top, there are navigation tabs: Port Access, Virtual Media, User Management, Device Settings, Security, Maintenance (selected), and Diagnostics. Below the tabs is a breadcrumb trail: Home > Maintenance > Device Information. The page content is divided into two main sections:

Device Information

Model:	DKX2-416
Hardware Revision:	0x44
Firmware Version:	2.0.0.2.5418
Serial Number:	HK(C6B00016
MAC Address:	00:0a:5d:01:33:c1

CIM Information

Port	Name	Type	Firmware Version	Serial Number
1	Dominion-KX2_Port1	VM	2A36	HJNV7250771
3	Dominion-KX2_Port3	PCIM	N/A	GNFFFFFFFFFFFF7565
8	Dominion-KX2_Port8	PowerStrip	00B2	PQ16A00058

Figure 1: Device Information

The following information is provided about the Dominion KX II: Model, Hardware Revision, Firmware Version, Serial Number, and MAC Address.

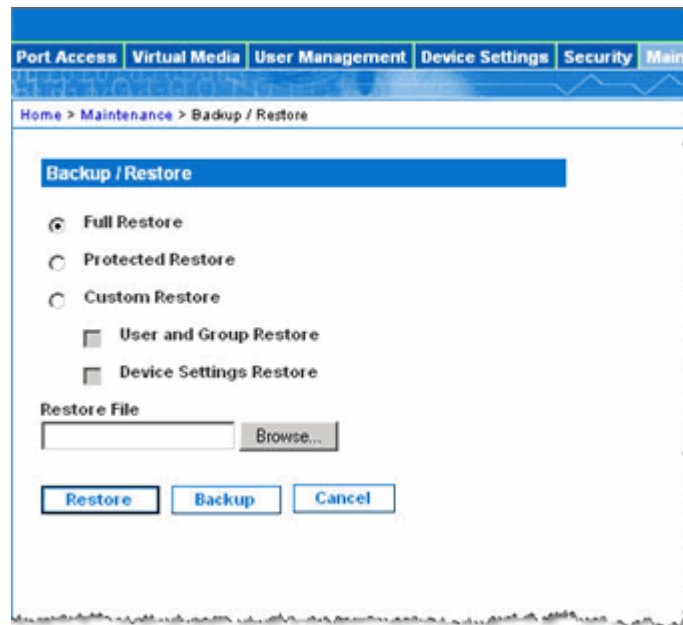
The following information is provided about the CIMs in use: Port (number), Name, Type (of CIM: DCIM, PCIM, Power Strip, or VM), Firmware Version, and Serial Number.

Backup and Restore

From the Backup/Restore page, you can backup and restore the settings and configuration for your Dominion KX II. In addition to using backup and restore for business continuity purposes, you can use this feature as a time-saving mechanism. For instance, you can quickly provide access to your team from another Dominion KX II, by backing up the user configuration settings from the Dominion KX II in use and restoring those configurations to the new Dominion KX II. You can also setup one Dominion KX II and copy its configuration to multiple Dominion KX II devices.

➤ *To access the Backup/Restore page:*

- Choose Maintenance > Backup/Restore. The Backup/Restore page opens:



Note: Backups are always complete system backups. Restores can be complete or partial depending on your selection.

➤ *To backup your Dominion KX II:*

1. Click Backup. A File Download dialog opens.
2. Click Save. A Save As dialog opens.
3. Choose the location, specify a file name, and click Save. A Download Complete dialog opens.

4. Click Close. The backup file is saved locally on your client machine with the name and location specified.

➤ *To restore your Dominion KX II:*

WARNING: Please exercise caution when restoring your Dominion KX II to an earlier version. Usernames and password in place at the time of the backup will be restored. If you do not remember the old administrative usernames and passwords, you will be locked out of the Dominion KX II.

In addition, if you used a different IP Address at the time of the backup, that IP Address will be restored as well. If the configuration uses DHCP, you may want to perform this operation only when you have access to the local port to check the IP address after the update.

1. Choose the type of restore you want to run:
 - Full Restore. A complete restore of the entire system; generally used for traditional backup and restore purposes.
 - Protected Restore. Everything is restored except device-specific information such as serial number, MAC Address, IP Address, name, etc. With this option, you can setup one Dominion KX II and copy the configuration to multiple Dominion KX II devices.
 - Custom Restore. With this option, you can select User and Group Restore, Device Settings Restore, or both. Select the appropriate checkboxes:
 - User and Group Restore. This option includes only user and group information. Use this option to quickly set up users on a different Dominion KX II.
 - Device Settings Restore. This option includes only device settings. Use this option to quickly copy the device information.
2. Click the Browse button. A Choose File dialog opens.
3. Navigate to and select the appropriate backup file and click Open. The file selected is listed in the Restore File field.
4. Click Restore. The configuration (based on the type of restore selected) is restored.

CIM Upgrade

Use this procedure to upgrade CIMs using the firmware versions stored in the memory of your Dominion KX II unit. In general, all CIMs are upgraded when you upgrade the device firmware using the Firmware Upgrade page. Use the CIM Upgrade page to upgrade new CIMs.

Note: Only D2CIM-VUSB can be upgraded from this page.

➤ *To upgrade CIMs using the Dominion KX II memory:*

1. Choose Maintenance > CIM Firmware Upgrade. The CIM Upgrade from Dominion KX II Flash page opens.
2. The Port (number), Name, Type, Current CIM Version, and Upgrade CIM Version are displayed for easy identification of the CIMs.
3. Select the Selected checkbox for each CIM you want to upgrade.

Tip: Use the Select All and Deselect All buttons to quickly select all (or deselect all) of the CIMs.

4. Click the Upgrade button. You are prompted to confirm the upgrade.
5. Click OK to continue the upgrade. Progress bars are displayed during the upgrade. Upgrading takes approximately 2 minutes (or less) per CIM.

➤ *To exit without upgrading:*

- Click Cancel.

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

Important: Do not turn off your Dominion KX II unit or disconnect CIMs while the upgrade is in progress - doing so will likely result in damage to the unit or CIMs.

➤ *To upgrade your Dominion KX II unit:*

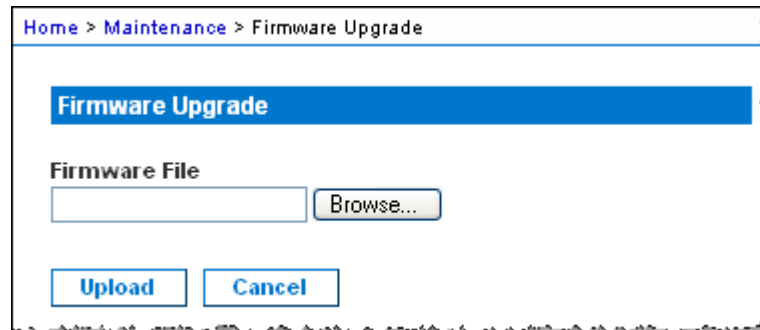
1. Locate the appropriate Raritan firmware distribution file (*.RFP), found on the Raritan Firmware Upgrades Web page:
<http://www.raritan.com/support/firmwareupgrades> and download the file.

CIM Upgrade

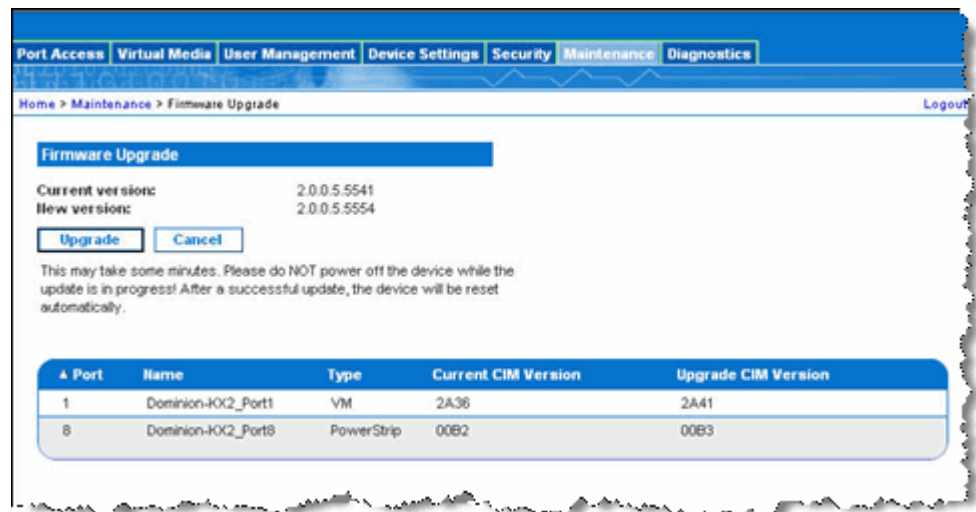
- Unzip the file. Please read all instructions included in the firmware ZIP files carefully before upgrading.

Note: Copy the firmware update file to a local PC before uploading. Do not load the file from a network drive.

- Choose Maintenance > Firmware Upgrade. The Firmware Upgrade page opens:



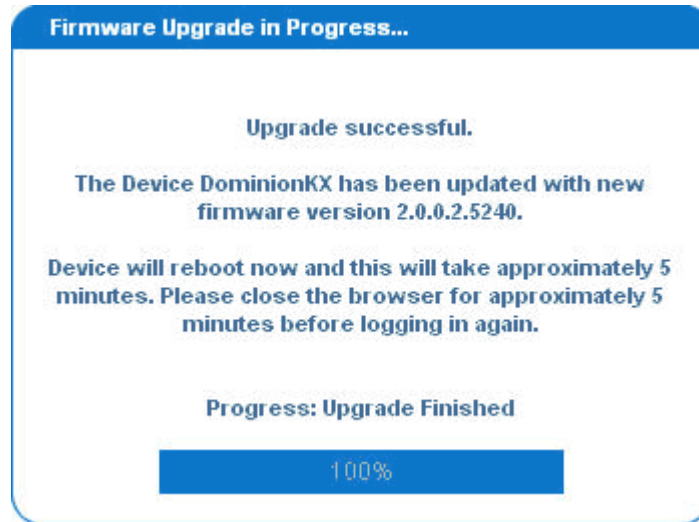
- Click the Browse button to navigate to the directory where you unzipped the upgrade file.
- Select the Review CIM Version Information? checkbox if you would like information displayed about the versions of the CIMs in use.
- Click Upload from the Firmware Upgrade page. Information about the upgrade and version numbers is displayed for your confirmation (if you opted to review CIM information, that information is displayed as well):



Port	Name	Type	Current CIM Version	Upgrade CIM Version
1	Dominion-IX2_Port1	VM	2A36	2A41
8	Dominion-IX2_Port8	PowerStrip	00B2	00B3

Note: At this point, connected users are logged out, and new login attempts are blocked.

7. Click Upgrade. Please wait for the upgrade to complete. Status information and progress bars are displayed during the upgrade. Upon completion of the upgrade, the unit reboots (1 beep sounds to signal that the reboot has completed).



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

For information about upgrading the device firmware using the Multi-Platform Client, refer to the Raritan Multi-Platform Client (MPC) and Raritan Remote Client (RRC) User Guide.

Upgrade History

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

- *To view the upgrade history:*
 - Choose Maintenance > Upgrade History. The Upgrade History page opens:

[Home](#) > Upgrade History

[Logout](#)

Upgrade History

Type	User	IP	Start Time	End Time	Previous Version	Upgrade Version	CIM's	Result
Full Firmware Upgrade	admin	192.168.59.105	October 22, 2007 10:14	October 22, 2007 10:21	1.0.0.1.6127	1.0.0.2.6178	show	Successful
Full Firmware Upgrade	admin	192.168.59.124	October 10, 2007 15:55	October 10, 2007 16:02	1.0.0.1.9999	1.0.0.1.6127	show	Successful

Reboot

Information is provided about the Dominion KX II upgrade(s) that have been run, the final status of the upgrade, the start and end times, and the previous and current firmware versions. Information is also provided about the CIMS, which can be obtained by clicking the show link for an upgrade. The CIM information provided is:

- Port. The port where the CIM is connected.
- Type. The type of CIM.
- Result. The result of the upgrade (success or fail).
- Current Version. The CIM firmware version.

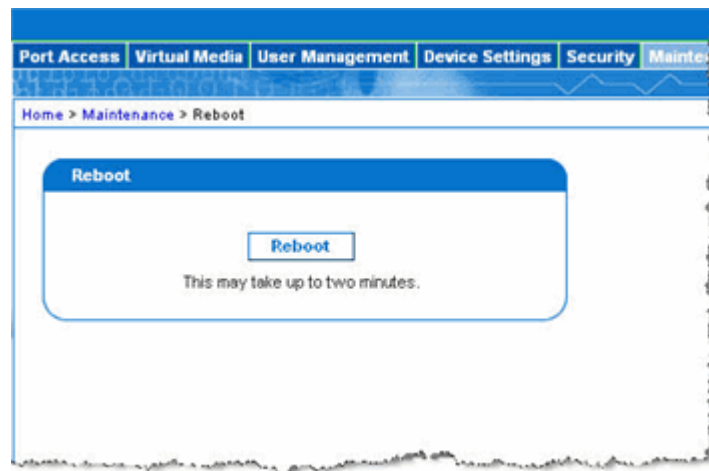
Reboot

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

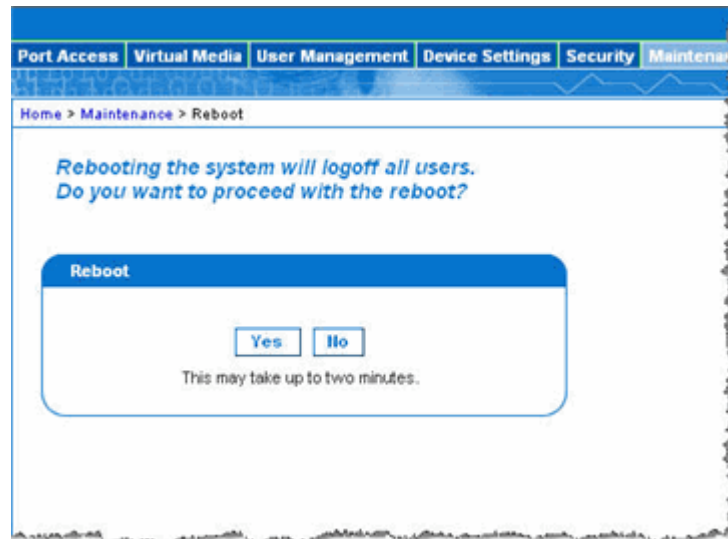
Important: All KVM and serial connections will be closed and all users will be logged off.

➤ *To reboot your Dominion KX II:*

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



2. Click the Reboot button. You are prompted to confirm the action:



3. Click Yes to proceed with the reboot.

➤ *To exit without rebooting:*

- Click No.

Chapter 13 Diagnostics

In This Chapter

Diagnostics Menu	174
Network Interface Page	175
Network Statistics Page	175
Ping Host Page.....	178
Trace Route to Host Page.....	179
Device Diagnostics.....	180

Diagnostics Menu

The Diagnostics pages are used for troubleshooting and are intended primarily for the administrator of the Dominion KX II device. All of the Diagnostics pages (except Device Diagnostics) run standard networking commands; the information displayed is the output of those commands.

The following Diagnostics menu options help you debug and configure the network settings:

- Network Interface
- Network Statistics
- Ping Host
- Trace Route to Host

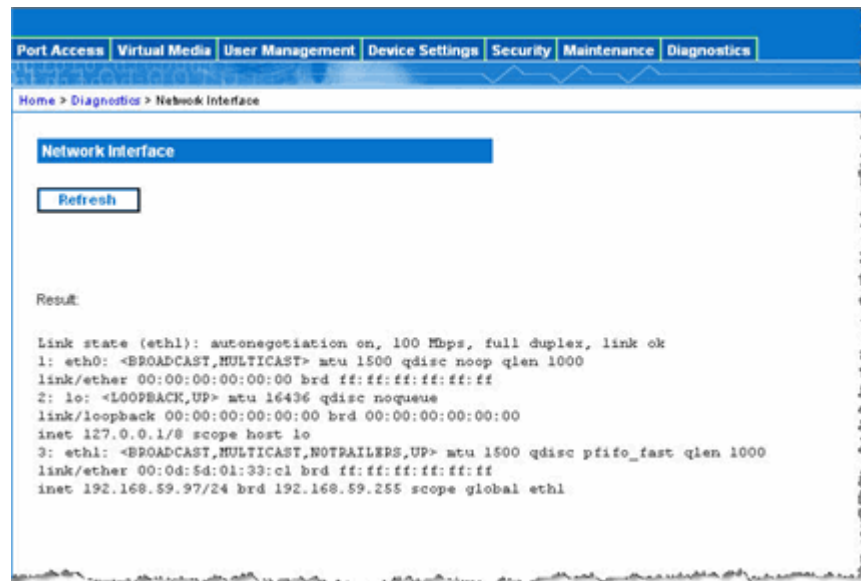
The Device Diagnostics option is intended for use in conjunction with Raritan Technical Support.

Use:	To:
Network Interface	Obtain the status of network interface.
Network Statistics	Obtain statistics about the network.
Ping Host	Determine whether a particular host is reachable across an IP network.
Trace Route to Host	Determine the route taken all the way to the selected host.
Device Diagnostics	Use when directed by Raritan Technical Support (Remote Console only).

Network Interface Page

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

- *To view information about your network interface:*
 - Choose Diagnostics > Network Interface. The Network Interface page opens:



The following information is displayed:

- Whether the Ethernet interface is up or down.
 - Whether the gateway is ping-able or not.
 - The LAN port that is currently active.
- *To refresh this information:*
 - Click the Refresh button.

Network Statistics Page

The Dominion KX II provides statistics about your network interface.

- *To view statistics about your network interface:*
 1. Choose Diagnostics > Network Statistics. The Network Statistics page opens.
 2. Choose the appropriate option from the Options drop-down list:

Network Statistics Page

- Statistics. Produces a page similar to the one displayed here:

The screenshot shows the 'Network Statistics' page in a web interface. The top navigation bar includes 'Port Access', 'Virtual Media', 'User Management', 'Device Settings', and 'Security'. The breadcrumb trail is 'Home > Diagnostics > Network Statistics'. The 'Options:' dropdown is set to '--statistics', and the 'Refresh' button is visible. The 'Result:' section displays the following statistics:

```
Ip:
8803 total packets received
0 forwarded
0 incoming packets discarded
8802 incoming packets delivered
8522 requests sent out
Icmp:
0 ICMP messages received
0 input ICMP message failed.
ICMP input histogram:
0 ICMP messages sent
0 ICMP messages failed
ICMP output histogram:
Tcp:
6 active connections openings
849 passive connection openings
0 failed connection attempts
15 connection resets received
1 connections established
7942 segments received
8304 segments send out
0 segments retransmited
0 bad segments received.
0 resets sent
Udp:
233 packets received
```

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

The screenshot shows the 'Network Statistics' page in a web interface. The top navigation bar includes 'Port Access', 'Virtual Media', 'User Management', 'Device Settings', 'Security', 'Maintenance', and 'Diagnostics'. The breadcrumb trail is 'Home > Diagnostics > Network Statistics'. The 'Options:' dropdown is set to '--interfaces', and the 'Refresh' button is visible. The 'Result:' section displays the following statistics:

```
Kernel Interface table
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth1 1500 0 13828 0 0 0 8680 0 0 0 B1NRU
lo 16436 0 196 0 0 0 196 0 0 0 LRU
```

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

Port Access Virtual Media User Management Device Settings Security Maint.

Home > Diagnostics > Network Statistics

Network Statistics

Options:

--route

Refresh

Result:

```
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
192.168.59.0 * 255.255.255.0 U 0 0 0 eth1
default 192.168.59.126 0.0.0.0 UG 0 0 0 eth1
```

3. Click the Refresh button.

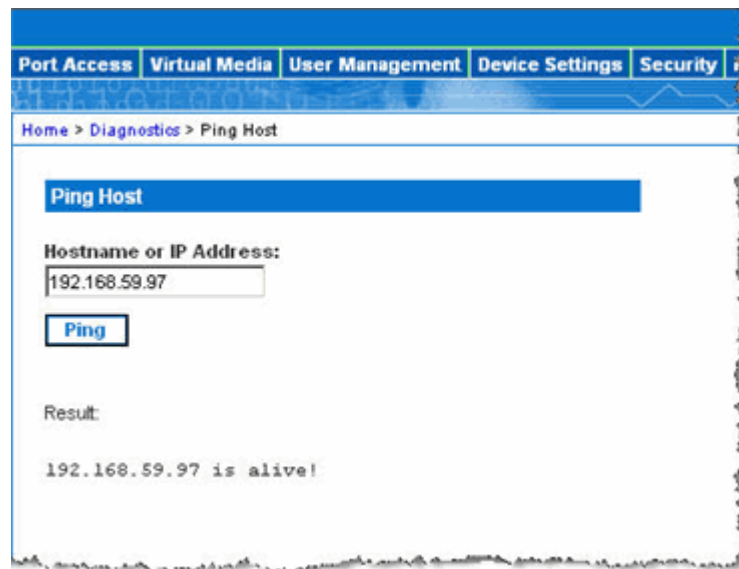
The relevant information is displayed in the Result field.

Ping Host Page

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

➤ *To ping the host:*

1. Choose Diagnostics > Ping Host. The Ping Host page opens:



2. Type either the hostname or IP Address into the Hostname or IP Address field.
3. Click Ping. The results of the ping are displayed in the Result field.

Trace Route to Host Page

Trace Route is a network tool used to determine the route taken all the way to the provided hostname or IP Address.

➤ *To trace the route to the host:*

1. Choose Diagnostics > Trace Route to Host. The Trace Route to Host page opens:

Port Access Virtual Media User Management Device Settings Security Maintenance

Home > Diagnostics > Trace Route to Host

Trace Route to Host

Hostname or IP Address:

Maximum Hops:

[Trace Route](#)

Result:

```
traceroute started wait for 2mins....  
1 192.168.59.97 (192.168.59.97) 0.438 ms 0.434 ms 0.368 ms
```

2. Type either the Hostname or IP Address into the Hostname or IP Address field.
3. Choose the Maximum Hops from the drop-down list (5 to 50 in increments of 5).
4. Click the Trace Route button. The trace route command is executed for the given hostname or IP Address and the maximum hops. The output of trace route is displayed in the Result field.

Device Diagnostics

Note: This page is for use by Raritan Field Engineers or when you are directed by Raritan Technical Support.

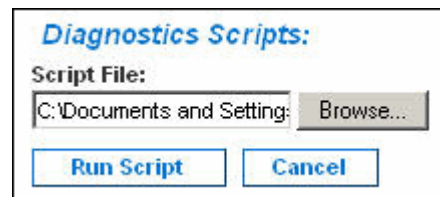
Device Diagnostics downloads the diagnostics information from Dominion KX II to the client machine. Three operations can be performed on this page:

- **Diagnostics Scripts.** Execute a special script provided by Raritan Technical Support during a critical error debugging session. The script is uploaded to the unit and executed. Once this script has been executed, you can download the diagnostics messages through the Save to File button.
- **Device Diagnostic Log.** Download the snapshot of diagnostics messages from the Dominion KX II unit to the client. This encrypted file is then sent to Raritan Technical Support; only Raritan can interpret this file.

Note: This page is accessible only by users with administrative privileges.

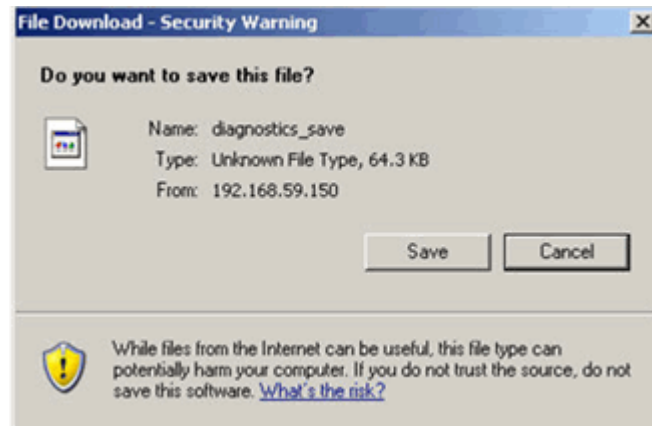
➤ *To run the Dominion KX II System diagnostics:*

1. Choose Diagnostics > Dominion KX II Diagnostics. The Dominion KX II Diagnostics page opens.
2. To execute a diagnostics script file emailed to you from Raritan Technical Support:
 - a. Retrieve the diagnostics file supplied by Raritan and unzip as necessary.
 - b. Use the Browse button. A Choose File dialog box opens.
 - c. Navigate to and select this diagnostics file.
 - d. Click Open. The file is displayed in the Script File field:



- e. Click Run Script.
 - f. Sent this file to Raritan Technical Support using step 4.
3. To create a diagnostics file to send to Raritan Technical Support:

- a. Click the Save to File button. The File Download dialog opens:



- b. Click Save. The Save As dialog box opens.
- c. Navigate to the desired directory and click Save.
- d. Email this file as directed by Raritan Technical Support.

Chapter 14 Dominion KX II Local Console

In This Chapter

- Dominion KX II Local Console183
- Starting the Dominion KX II Local Console.....185
- Accessing KVM Target Servers.....187
- Local Port Administration.....189

Dominion KX II Local Console

Dominion KX II provides at-the-rack access and administration via its local port, which features a browser-based graphical user interface for quick, convenient switching between servers. The Dominion KX II Local Console provides a direct analog connection to your connected servers; the performance is as if you were directly connected to the server's keyboard, mouse, and video ports. The Dominion KX II Local Console provides the same administrative functionality as the Dominion KX II Remote Console.

The Dominion KX II Local Console supports the following language keyboards: US English, UK English, German, French, Norwegian, Swedish, Danish, Belgium, Japanese, Korean, Simplified Chinese, and Traditional Chinese.

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

The screenshot displays the Dominion KX II Local Console web interface. The top navigation bar includes links for Port Access, User Management, Device Settings (selected), Security, Maintenance, and Diagnostics. The main content area is divided into two columns. The left column contains a sidebar with sections: Time & Session (May 02, 2007 10:06:59), User: admin, State: 36 min idle, Your IP: Local Console, Last Login: May 02, 2007 04:11; Device Information (Device Name: DominionKX, IP Address: 192.168.59.124, Firmware: 2.0.0.5.5541, PowerIn1: on, PowerIn2: off); Port States (2 Ports up, 13 Ports down, 14 Ports idle, 1 Ports busy); and Connected Users (admin (Local Console) 36 min idle, admin (192.168.59.65) RC active). The right column contains two main sections: Network Basic Settings and Network Miscellaneous Settings. The Network Basic Settings section includes fields for Device Name (DominionKX), IP auto configuration (DHCP), Preferred host name (DHCP only), IP address (192.168.59.124), Subnet mask (255.255.255.0), Gateway IP address (192.168.59.126), Primary DNS server IP address (192.168.59.2), and Secondary DNS server IP address (192.168.51.10). The Network Miscellaneous Settings section includes Discovery Port (5000), Bandwidth Limit (No Limit), LAN Interface Settings (Autodetect), Current LAN interface parameters (autonegotiation on, 100 Mbps, full duplex, link ok), LAN Interface Speed & Duplex (Autodetect), Enable Automatic Failover (checkbox), Ping Interval (seconds) (30), Timeout (seconds) (60), and a Set System ACL button. At the bottom of the Network Basic Settings section are buttons for OK, Reset to defaults, and Cancel.

Physical Connections

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



Monitor: Attach a standard multi-sync VGA monitor to the HD15 (female) video port.

Keyboard: Attach either a standard PS/2 keyboard to the Mini-DIN6 (female) keyboard port, or a standard USB keyboard to one of the USB Type A (female) ports.

Mouse: Attach either a standard PS/2 mouse to the Mini-DIN6 (female) mouse port or a standard USB mouse to one of the USB Type A (female) ports.

Reset Button

At the back of the Dominion KX II unit, there is a Reset button. It is recessed to prevent accidental presses (you will need a pointed object to use this button).

The actions that are performed when the reset button is pressed are defined in the graphical user interface. Refer to ***Security Settings, Encryption & Share*** (see "Encryption & Share" on page 157) for more information.

*Note: It is recommended that you save the audit log prior to performing a factory reset. The audit log is deleted when a factory reset is performed and the reset event is not logged in the audit log. For more information about saving the audit log, please refer to **Audit Log** (on page 164).*

➤ *To reset the unit:*

1. Power off the Dominion KX II unit.
2. Use a pointed object to press and hold the reset button.
3. While continuing to hold the reset button, power the Dominion KX II unit back on.

4. Continue holding the reset button for 5-10 seconds. Once the unit has been reset; two short beeps signal completion.



Starting the Dominion KX II Local Console

Simultaneous Users

The Dominion KX II Local Console provides an independent access path to the connected KVM target servers. Using the Local Console does not prevent other users from simultaneously connecting over the network. And even when remote users are connected to Dominion KX II, you can still simultaneously access your servers from the rack via the Local Console.

Security and Authentication

In order to use the Dominion KX II Local Console, you must first authenticate with a valid username and password. Dominion KX II provides a fully-integrated authentication and security scheme, whether your access is via the network or the local port. In either case, Dominion KX II allows access only to those servers to which a user has access permissions (refer to **User Management** (on page 100) for additional information on specifying server access and security settings).

If your Dominion KX II has been configured for external authentication services (LDAP/LDAPS, RADIUS, or Active Directory), authentication attempts at the Local Console also are authenticated against the external authentication service.

Note: You can also specify no authentication for local console access; this option is recommended only for secure environments.

➤ To use the Dominion KX II Local Console:

1. You need a keyboard, mouse, and video display connected to the local ports at the back of the Dominion KX II unit. Refer to **Physical Connections** (on page 184) for more information about the local port connections.
2. Start the Dominion KX II unit; the Dominion KX II Local Console interface displays.

Dominion KX II Local Console Interface

The Dominion KX II Local Console interface is almost identical to the Dominion KX II Remote Console interface. Where there are differences, they are noted in the user manual. Refer to User Interfaces, **Console** (see "Dominion KX II Local Console: Dominion KX II Devices" on page 42), and **Console Menu Tree** (see "Dominion KX II Console Menu Tree" on page 49) for additional information.

Available Resolutions

The Dominion KX II Local Console provides the following resolutions to support various monitors:

- 800x600
- 1024x768
- 1280x1024

Each of these resolutions supports a refresh rate of 60Hz and 75Hz.

Accessing KVM Target Servers

Server Display

After you login to the Dominion KX II Local Console, the **Port Access** page opens. This page lists all of the Dominion KX II ports, the connected KVM target servers, and their status and availability.

Raritan. Local Console Port

Port Access User Management Device Settings Security Maintenance Diagnostics

Home > Port Access Logout

Port Access

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

Port Number	Port Name	Status	Availability
1	Dominion-KX2_Port1	down	idle
2	Dominion-KX2_Port2	down	idle
3	UPmachine	up	busy
4	Dominion-KX2_Port4	down	idle
5	Dominion-KX2_Port5	down	idle
6	Dominion-KX2_Port6	down	idle
7	Dominion-KX2_Port7	down	idle
8	Dominion-KX2_Port8	up	idle
9	Dominion-KX2_Port9	down	idle
10	Dominion-KX2_Port10	down	idle
11	Dominion-KX2_Port11	down	idle
12	Dominion-KX2_Port12	down	idle
13	Dominion-KX2_Port13	down	idle
15	Dominion-KX2_Port15	down	idle
16	Dominion-KX2_Port16	down	idle

Copyright © 2007 Raritan Computer Inc.

Time & Session:
March 02, 2007 14:27:49
User: admin
State: active
Your IP: Local Console
Last Login: Mar 02, 2007 14:12

Device Information:
Device Name: DominionKX
IP Address: 192.168.59.97
Firmware: 2.0.0.2.5282
PowerIn1: on
PowerIn2: off

Port States:
2 Ports up
13 Ports down
14 Ports idle
1 Ports busy

Connected Users:
admin (Local Console)
active
admin (192.168.59.93)
RC active

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

- **Port Number.** Numbered from 1 to the total number of ports available for the Dominion KX II unit. Please note that ports connected to power strips will not be among those listed, resulting in gaps in the Port Number sequence.
- **Port Name.** The name of the Dominion KX II port; initially set to Dominion KX II-Port#, but you can change the name to something more descriptive. When you click on the Port Name link, an Action Menu is opened. Refer to the **Port Action Menu** (on page 61) for more information about the menu options available.

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

Accessing KVM Target Servers

- Status. The Status is either up or down.
 - Availability. Valid Values per include Idle, Connected, Busy, or Unavailable.
- *To change the sort order:*
- Click the column heading you want to sort on. The list of KVM target servers is sorted by that column.

Hotkeys

Because the Dominion KX II Local Console interface is completely replaced by the interface for the target server you are accessing, a hotkey is utilized so you can switch between these interfaces.

The Local Port hotkey allows you to rapidly access the Dominion KX II Local Console user interface when a target server is currently being viewed. The default is to press the Scroll Lock key twice in rapid succession, but you can designate another key combination (available in the Local Port Settings page) as the hotkey. Refer to **Local Port Settings** (see "Local Port Settings (Dominion KX II Local Console Only)" on page 190) for more information.

Accessing a Target Server

- *To access a target server:*
1. Click the Port Name of the target you want to access. The Port Action Menu is displayed.
 2. Choose Connect from the **Port Action Menu** (on page 61). The video display switches to the target server interface.

Returning to the Dominion KX II Local Console Interface

Important: The Dominion KX II Local Console default hotkey is to press the Scroll Lock key twice rapidly. This key combination can be changed in the *Local Port Settings* (see "Local Port Settings (Dominion KX II Local Console Only)" on page 190) page.

- *To return to the Dominion KX II Local Console from the target server:*
- Press the hotkey (default is Scroll Lock) twice rapidly. The video display switches from the target server interface to the Dominion KX II Local Console interface.

Local Port Administration

The Dominion KX II can be managed by either the Dominion KX II Local Console or the Dominion KX II Remote Console. Please note that the Dominion KX II Local Console also provides access to these administrative functions:

- Local Port Settings
- Factory Reset

Note: Only users with administrative privileges can access these functions.

Local Port Administration

Local Port Settings (Dominion KX II Local Console Only)

From the Local Port Settings page, you can customize many settings for the Dominion KX II Local Console including keyboard, local port hotkey, video switching delay, power save mode, local user interface resolution settings, and local user authentication.

Note: This feature is available only on the Dominion KX II Local Console.

➤ To configure the local port settings:

1. Choose Device Settings > Local Port Settings. The Local Port Settings page opens:

The screenshot shows a web browser window with the address bar displaying 'Home > Device Settings > Local Port Settings' and a 'Logout' link in the top right corner. The main content area is titled 'Local Port Settings' in a blue header. Below the header, a note states: 'Note: Any changes to the Local Port Settings will restart the browser.' The settings are organized into several sections: 'Keyboard Type' with a dropdown menu set to 'US'; 'Local Port Hotkey' with a dropdown menu set to 'Double Click Scroll Lock'; 'Video Switching Delay (in secs)' with a text input field set to '0'; 'Power Save Mode' with an unchecked checkbox; 'Power Save Mode Timeout (in minutes)' with a text input field set to '10'; 'Resolution' with a dropdown menu set to '1024x768'; 'Refresh Rate (Hz)' with a dropdown menu set to '60 Hz'; and 'Local User Authentication' with three radio buttons ('Local/LDAP/RADIUS' is selected), a 'None' option, and a checked checkbox for 'Ignore CC managed mode on local port'. At the bottom of the form are three buttons: 'OK', 'Reset to defaults', and 'Cancel'. The footer of the page reads 'Copyright © 2007 Raritan Computer Inc.'

2. Choose the appropriate Keyboard Type from among the options in the drop-down list:
 - US
 - US/International
 - UK

- French
 - German
 - JIS (Japanese Industry Standard)
 - Simplified Chinese
 - Traditional Chinese
 - Dubeolsik Hangul (Korean)
 - German
 - Norwegian
 - Swedish
 - Danish
 - Belgian
3. Choose the Local Port Hotkey. The Local Port Hotkey is used to return to the Dominion KX II Local Console interface when a target server interface is being viewed. The default is Double Click Scroll Lock, but you can select any key combination from the drop-down list:

Hotkey:	Take this Action:
Double Click Scroll Lock	Press Scroll Lock key twice quickly
Double Click Num Lock	Press Num Lock key twice quickly
Double Click Caps Lock	Press Caps Lock key twice quickly
Double Click Left Alt key	Press the left Alt key twice quickly
Double Click Left Shift key	Press the left Shift key twice quickly
Double Click Left Ctrl key	Press the left Ctrl key twice quickly

4. Set the Video Switching Delay from 0 - 5 seconds, if necessary. Generally 0 is used unless more time is needed (certain monitors require more time to switch the video).
5. If you would like to use the power save feature:
- a. Select the Power Save Mode checkbox.
 - b. Set the amount of time (in minutes) in which Power Save Mode will be initiated.
6. Choose the Resolution for the Dominion KX II Local Console from the drop-down list:
- 800x600

Local Port Administration

- 1024x768
 - 1280x1024
7. Choose the Refresh Rate from the drop-down list:
 - 60 Hz
 - 75 Hz
 8. Choose the type of Local User Authentication:
 - Local/LDAP/LDAPS/RADIUS. This is the recommended option; for more information about authentication, refer to *Remote Authentication* (on page 37) and *Authentication vs. Authorization* (on page 38).
 - None. There is no authentication for local console access. This option is recommended for secure environments only.
 9. Select the Ignore CC managed mode on local port checkbox if you would like local user access to the Dominion KX II even when the device is under CC-SG management.

Note: If you clear this checkbox but then want local port access, you will have to remove the device from under CC-SG management (from within CC-SG) and then you will be able to check this checkbox.

10. Click OK.
- *To close the page without saving any changes:*
 - Click Cancel.
 - *To reset back to defaults:*
 - Click Reset to Defaults.

Factory Reset (Dominion KX II Local Console Only)

Note: This feature is available only on the Dominion KX II Local Console.

The Dominion KX II offers several types of reset modes from the Local Console user interface.

*Note: It is recommended that you save the audit log prior to performing a factory reset. The audit log is deleted when a factory reset is performed and the reset event is not logged in the audit log. For more information about saving the audit log, please refer to **Audit Log** (on page 164).*

➤ *To perform a factory reset:*

1. Choose Maintenance > Factory Reset. The Factory Reset page opens.
2. Choose the appropriate reset option.
 - **Full Factory Reset:** Removes the entire configuration and resets the unit completely to the factory defaults. Please note that any management associations with CommandCenter will be broken. Because of the complete nature of this reset, you will be prompted to confirm the factory reset.
 - **Network Parameter Reset:** Resets the network parameters (from Device Settings > Network Settings) of the unit back to the default values:
 - IP auto configuration
 - IP Address
 - Subnet Mask
 - Gateway IP address
 - Primary DNS server IP address
 - Secondary DNS server IP address
 - Discovery Port
 - Bandwidth Limit
 - LAN Interface Speed & Duplex
 - Enable Automatic Failover
 - Ping Interval (seconds)
 - Timeout (Seconds)

You will be prompted to confirm this action because all network settings will be permanently lost.

1. Click Reset to continue. You will be prompted to confirm the factory reset.

Local Port Administration

2. Click the Really Reset button to proceed. Upon completion, the Dominion KX II unit is automatically restarted.

Appendix A Specifications

In This Chapter

Environmental Requirements	195
Remote Connection	198
TCP and UDP Ports Used	199
Target Server Connection Distance and Video Resolution	200
Network Speed Settings.....	201

Environmental Requirements

Operating	
Temperature	0°C- 40°C (32°F - 104°F)
Humidity	20% - 85% RH
Altitude	N/A
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A
Non-Operating	
Temperature	0°C- 50°C (32°F - 122°F)
Humidity	10% - 90% RH
Altitude	N/A
Vibration	5-55-5 HZ, 0.38mm, 1 minutes per cycle; 30 minutes for each axis (X, Y, Z)
Shock	N/A

Physical Specifications

Environmental Requirements

Part Number	DKX2-108	DKX2-116	DKX2-132	DKX2-216	DKX2-232	DKX2-416	DKX2-432
Line Item Description	8-Port Dominion KX II with 1-user Network Access and Local Port; Virtual Media, Dual Power	16-Port Dominion KX II with 1-user Network Access and Local Port; Virtual Media, Dual Power	32-Port Dominion KX II with 1-user Network Access and Local Port; Virtual Media, Dual Power	16-Port Dominion KX II with 2-user Network Access and Local Port; Virtual Media, Dual Power	32-Port Dominion KX II with 2-user Network Access and Local Port; Virtual Media, Dual Power	16-Port Dominion KX II with 4-user Network Access and Local Port; Virtual Media, Dual Power	32-Port Dominion KX II with 4-user Network Access and Local Port; Virtual Media, Dual Power
Weight	8.58 lbs; 3.9kg	8.65 lbs; 3.9kg	9.0 lbs; 4.1kg	8.65 lbs; 3.9 kg	9.0 lbs; 4.1 kg	9.04 lbs; 4.1 kg	9.48 lbs; 4.3 kg
Product Dimensions (WxDxH)	1.75" x 17.32" x 11.4" 44mm x 439mm x 290mm	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm	1.75" x 17.3" x 11.4" 44mm x 439mm x 290mm
Shipping Weight	14.3 lbs; 6.5 kg	14.85 lbs; 6.7 kg	14.9 lbs; 6.8 kg	14.49 lbs; 6.6 kg	14.9 lbs; 6.8 kg	14.94 lbs; 6.8 kg	15.38 lbs; 7.0 kg
Shipping Dimensions (WxDxH)	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	22" x 16.6" x 6.5" 559mm x 422mm x 165mm	22" x 16.6" x 6.5" 559mm x 422mm x 165mm
UPC Code	7858136241 09	7858136240 55	7858136240 79	7858136240 86	785813625 021	7858136253 59	785813625 380
Power	Dual Power 100/240 V 50/60 Hz 0.6A 61.3 Watts	Dual Power 100/240 V 50/60 Hz 0.6A 25.4 Watts	Dual Power 100/240 V 50/60 Hz 0.6A 26 Watts	Dual Power 100/240 V 50/60 Hz 0.6A 26.3 Watts	Dual Power 100/240 V 50/60 Hz 0.6A 27 Watts	Dual Power 100/240 V 50/60 Hz 1A 62 Watts	Dual Power 100/240 V 50/60 Hz 1A 64 Watts

Computer Interface Modules (CIMs)

Part Number	D2CIM-VUSB	DCIM-PS2	DCIM-USB	DCIM-SUSB
Line Item Description	Dominion KX II Computer Interface Module [USB Port with Virtual Media]	Dominion KX I & II Computer Interface Module [PS/2 Port]	Dominion KX I & II Computer Interface Module [USB Port]	Dominion KX I & II Computer Interface Module [USB Port for Sun]
Product Weight	0.2 lbs	0.2 lbs	0.2 lbs	0.2 lbs
Product Dimensions (WxDxH)	1.3" x 3.0" x 0.6"	1.3" x 3.0" x 0.6"	1.3" x 3.0" x 0.6"	1.3" x 3.0" x 0.6"
Shipping Weight	0.2 lbs	0.2 lbs	0.2 lbs	0.2 lbs
Shipping Dimensions (WxDxH)	7.2" x 9" x 0.6"	7.2" x 9" x 0.6"	7.2" x 9" x 0.6"	7.2" x 9" x 0.6"
UPC Code	785813332004	785813338532	785813338518	785813338556

Part Number	DCIM-USBG2	DCIM-SUN	D2CIM-PWR	D2CIM-VUSB-32PAC	D2CIM-VUSB - 64PAC
Line Item Description	Dominion KX I & II Computer Interface Module [USB and Sun USB Port] G2 CIM	Dominion KX I & II Computer Interface Module [Sun Port, HD15 Video]	Dominion KX II Computer Interface Module for Remote Power strips	Bulk pack of 32 D2CIM-VUSB	Bulk pack of 64 D2CIM-VUSB
Product Weight	0.2 lbs	0.2 lbs	0.2 lbs	6.4 lb	12.8 lb
Product Dimensions (WxDxH)	1.3" x 3.0" x 0.6"	1.3" x 3.0" x 0.6"	1.3" x 3.0" x 0.6"	(1.3" x 3.0" x 0.6")*32	(1.3" x 3.0" x 0.6")*64
Shipping Weight	0.2 lbs	0.2 lbs	0.2 lbs	8.01 lb	18.13 lb
Shipping Dimensions (WxDxH)	7.2" x 9" x 0.6"	7.2" x 9" x 0.6"	7.2" x 9" x 0.6"	21.65"x12.20"x4.33"	22.64"x9.45"x12.99"
UPC Code	785813338884	785813338549	785813332011	785813332028	785813332035

Remote Connection

Remote Connection

Network: 10BASE-T, 100BASE-T, and 1000BASE-T (Gigabit)
Ethernet

Protocols: TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS,
LDAP/LDAPS

TCP and UDP Ports Used

- HTTP, Port 80 - All requests received by Dominion KX II via HTTP (port 80) are automatically forwarded to HTTPS for complete security. Dominion KX II responds to Port 80 for user convenience, relieving users from having to explicitly type “https://” in the URL field to access Dominion KX II, but while still preserving complete security.
- HTTPS, Port 443 - This port is used for a single purpose only: to send the Dominion KX II web-accessible clients (Dominion KX II Console, MPC) to the user. No other communication occurs on this port. If you do not wish to use the Dominion KX II web-access capabilities and instead prefer to use the installed client software provided on the CD-ROM, you can prevent access to Port 443 via your firewall and Dominion KX II can still function.
- Dominion KX II (Raritan KVM-over-IP) Protocol, Configurable Port 5000 - With the exception of the ports above, all communication to Dominion KX II occurs over a single, configurable TCP Port. By default, this is set to Port 5000, but you may configure it to use any TCP port of your choice (except 80 and 443). For details on how to configure this setting, refer to *Network Settings* (on page 124).
- SNTP (Time Server) on Configurable UDP Port 123 (optional) - Dominion KX II offers the optional capability to synchronize its internal clock to a central time server. This function requires the use of UDP Port 123 (the standard for SNTP), but can also be configured to use any port of your designation.
- LDAP/LDAPS on Configurable Ports 389 and 636 (optional) - If Dominion KX II is configured to remotely authenticate user logins via the LDAP/LDAPS protocol, ports 389 and 636 will be used, but the system can also be configured to use any port of your designation.
- RADIUS on Configurable Port 1812 (optional) - If Dominion KX II is configured to remotely authenticate user logins via the RADIUS protocol, either port 1812 or 1813 will be used, but the system can also be configured to use any port of your designation.
- RADIUS Accounting on Configurable Port 1813 - If Dominion KX II is configured to remotely authenticate user logins via the RADIUS protocol, and also employs RADIUS accounting for event logging, port 1813 or an additional port of your designation will be used to transfer log notifications.

Target Server Connection Distance and Video Resolution

- SYSLOG on Configurable UDP Port 514 - If Dominion KX II is configured to send messages to a Syslog server, then the indicated port(s) will be used for communication - uses UDP Port 514.
- SNMP Default UDP Ports (optional) - Port 161 is used for inbound/outbound read/write SNMP access and port 162 is used for outbound traffic for SNMP traps.
- UDP Port 21 - Port 21 is used for the Dominion KX II command line interface (when you are working with Raritan Technical Support).
- SSH - (Secure Shell) SSHv2 Server is configured to run on the Dominion KX II by default.
- Telnet - Telnet ports can be configured but are not recommended.

Target Server Connection Distance and Video Resolution

The maximum supported distance is a function of many factors including the type/quality of Cat 5 cable, server type and manufacturer, video driver and monitor, environmental conditions, and user expectations. The following table summarizes the maximum target server distance for various video resolutions and refresh rates:

Video Resolution	Refresh Rate	Maximum Distance
1600x1200	60	50 ft (15 m)
1280x1024	60	100 ft (30 m)
1024x768	60	150 ft (45 m)

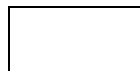
Due to the multiplicity of server manufacturers and types, OS versions, video drivers, etc. and the subjective nature of video quality, Raritan cannot guarantee performance across all distances in all environments.

Refer to the Supported Video Resolutions for the video resolutions supported by Dominion KX II.

Network Speed Settings

Dominion Dominion KX II Network Speed Setting							
Network Switch Port Setting		Auto	1000/Full	100/Full	100/Half	10/Full	10/Half
	Auto	Highest Available Speed	1000/Full	Dominion KX II: 100/Full Switch: 100/Half	100/Half	Dominion KX II: 10/Full Switch: 10/Half	10/Half
		1000/Full	1000/Full	No Communication	No Communication	No Communication	No Communication
	100/Full	Dominion KX II: 100/Half Switch: 100/Full	Dominion KX II: 100/Half Switch: 100/Full	100/Full	Dominion KX II: 100/Half Switch: 100/Full	No Communication	No Communication
	100/Half	100/Half	100/Half	Dominion KX II: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
	10/Full	Dominion KX II: 10/Half Switch: 10/Full	No Communication	No Communication	No Communication	10/Full	Dominion KX II: 10/Half Switch: 10/Full
		10/Half	No Communication	No Communication	No Communication	Dominion KX II: 10/Full Switch: 10/Half	10/Half
	10/Half	10/Half	No Communication	No Communication	No Communication	Dominion KX II: 10/Full Switch: 10/Half	10/Half
	10/Half	10/Half	No Communication	No Communication	No Communication	Dominion KX II: 10/Full Switch: 10/Half	10/Half

Legend:



Does not function, as expected

Network Speed Settings



Supported



Functions; not recommended



NOT supported by Ethernet specification; product will communicate, but collisions will occur



Per Ethernet specification, these should be “no communication”, however, note that the Dominion KX II behavior deviates from expected behavior

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

Appendix B Updating the LDAP Schema

Note: The procedures in this chapter should be attempted only by experienced users.

In This Chapter

Returning User Group Information	203
Setting the Registry to Permit Write Operations to the Schema	204
Creating a New Attribute	204
Adding Attributes to the Class	205
Updating the Schema Cache	207
Editing rcusergroup Attributes for User Members.....	208

Returning User Group Information

Use the information in this chapter to return User Group information (and assist with authorization) once authentication is successful.

From LDAP

When an LDAP/LDAPS authentication is successful, Dominion KX II determines the permissions for a given user based on the permissions of the user's group. Your remote LDAP server can provide these user group names by returning an attribute named as follows:

rcusergroup attribute type: string

This may require a schema extension on your LDAP/LDAPS server. Consult your authentication server administrator to enable this attribute.

From Microsoft Active Directory

Note: This should be attempted only by an experienced Active Directory administrator.

Returning user group information from Microsoft's Active Directory for Windows 2000 Server requires updating the LDAP/LDAPS schema. Refer to your Microsoft documentation for more detail.

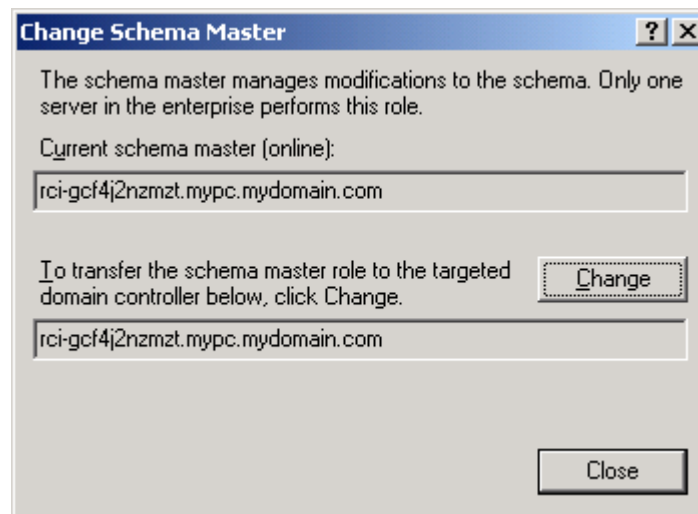
1. Install the schema plug-in for Active Directory - refer to Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

➤ *To permit write operations to the schema:*

1. Right-click the Active Directory Schema root node in the left pane of the window, and then click Operations Master. The Change Schema Master dialog opens:



2. (Optional) Select the checkbox before The Schema can be modified on this Domain Controller.
3. Click OK.

Creating a New Attribute

➤ *To create new attributes for the rcigroup class:*

1. Click the + symbol before Active Directory Schema in the left pane of the window.
2. Right-click Attributes in the left pane.

- Click New, and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute window opens.

Create New Attribute

Create a New Attribute Object

Identification

Common Name: rciusergroup

LDAP Display Name: rciusergroup

Unique X500 Object ID: 1.3.6.1.4.1.13742.50

Description: Raritan's LDAP attribute

Syntax and Range

Syntax: Case Insensitive String

Minimum: 1

Maximum: 24

☐ Multi-Valued

OK Cancel

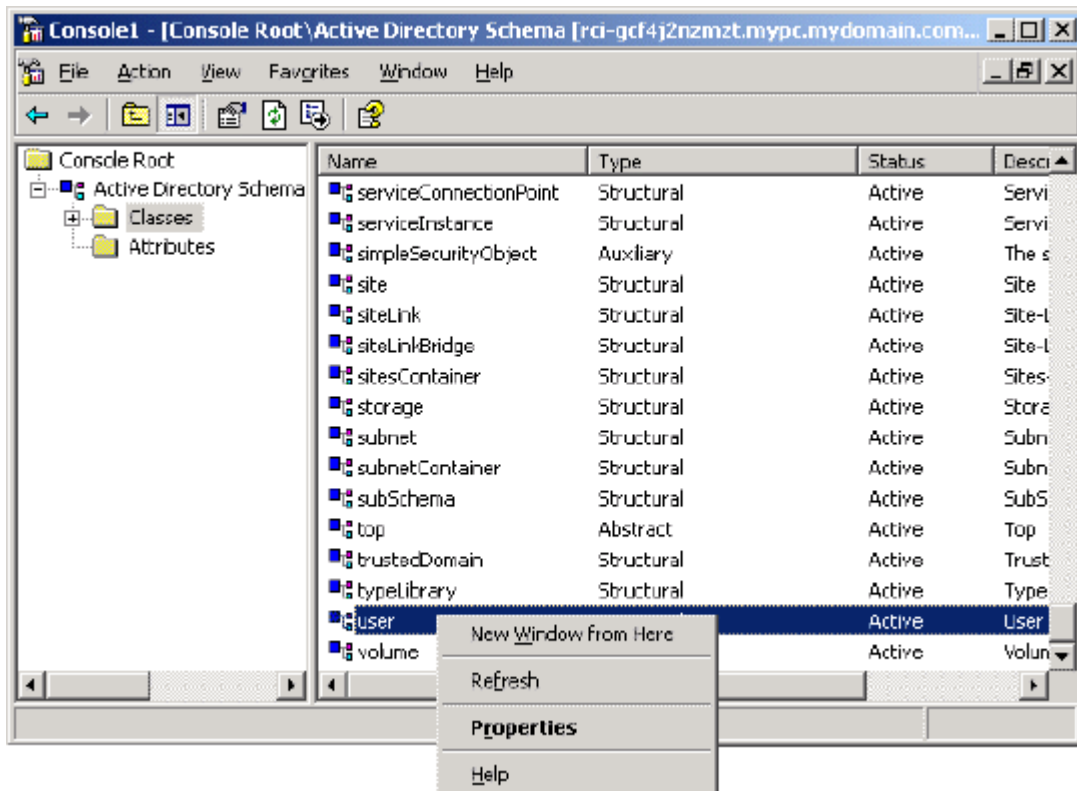
- Type rciusergroup in the Common Name field.
- Type rciusergroup in the LDAP Display Name field.
- Type 1.3.6.1.4.1.13742.50 in the Unique x5000 Object ID field.
- Type a meaningful description in the Description field.
- Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
- Type 1 in the Minimum field.
- Type 24 in the Maximum field.
- Click OK to create the new attribute.

Adding Attributes to the Class

- *To add attributes to the class:*
- Click Classes in the left pane of the window.

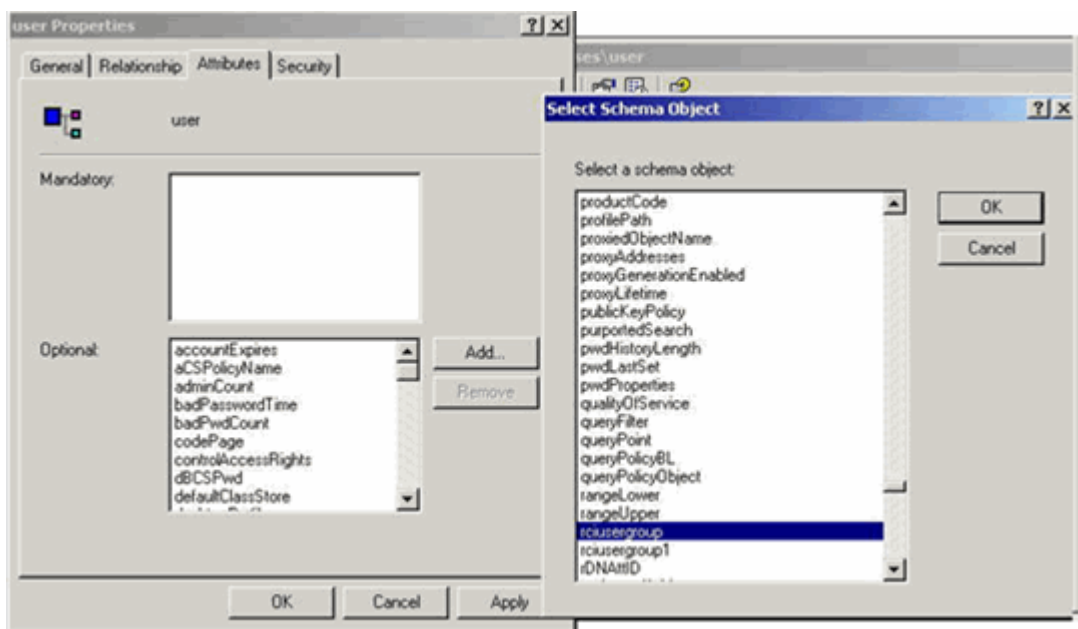
Adding Attributes to the Class

2. Scroll to the user class in the right pane, and right-click on it.



3. Choose Properties from the menu. The user Properties window appears.

4. Click on the Attributes tab to open it.



5. Click Add.
6. Choose rcusergroup from the Select Schema Object list.
7. Click OK in the Select Schema Object dialog.
8. Click OK in the user Properties dialog.

Updating the Schema Cache

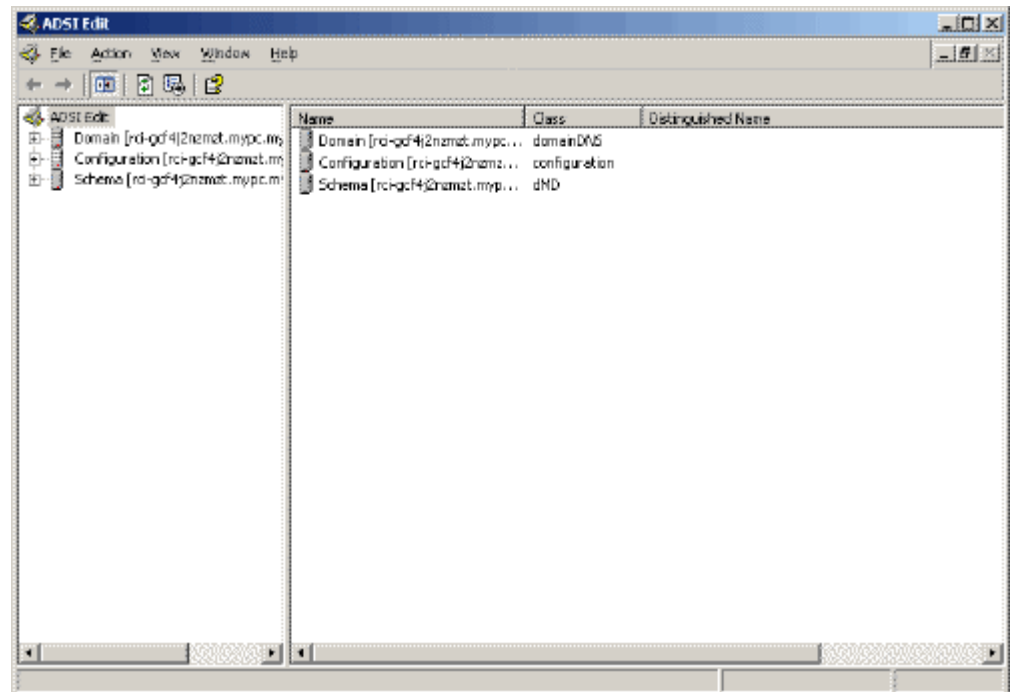
- *To update the schema cache:*
 1. Right-click Active Directory Schema in the left pane of the window and select Reload the Schema from the shortcut menu.
 2. Minimize the Active Directory Schema MMC (Microsoft Management Console) console.

Editing rcusergroup Attributes for User Members

To run Active Directory script on Windows 2003 server, please use the script provided by Microsoft (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

➤ *To edit the individual user attributes within the group rcusergroup:*

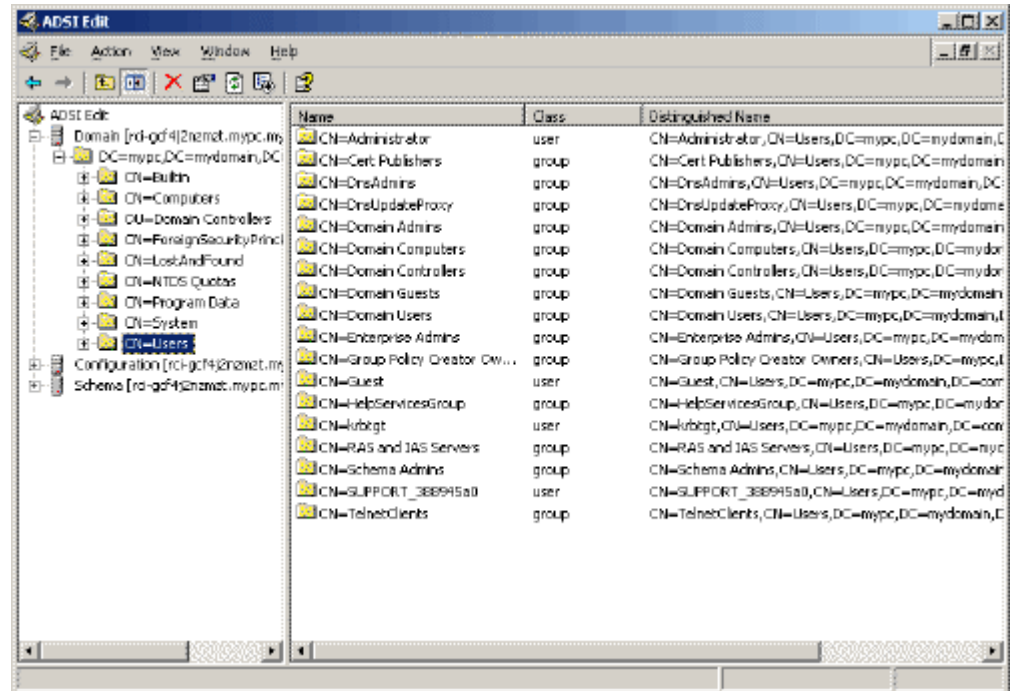
1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.
3. Go to the directory where the support tools were installed.
4. Run adsiedit.msc. The ADSI Edit window opens.



5. Open the Domain.

Appendix B: Updating the LDAP Schema

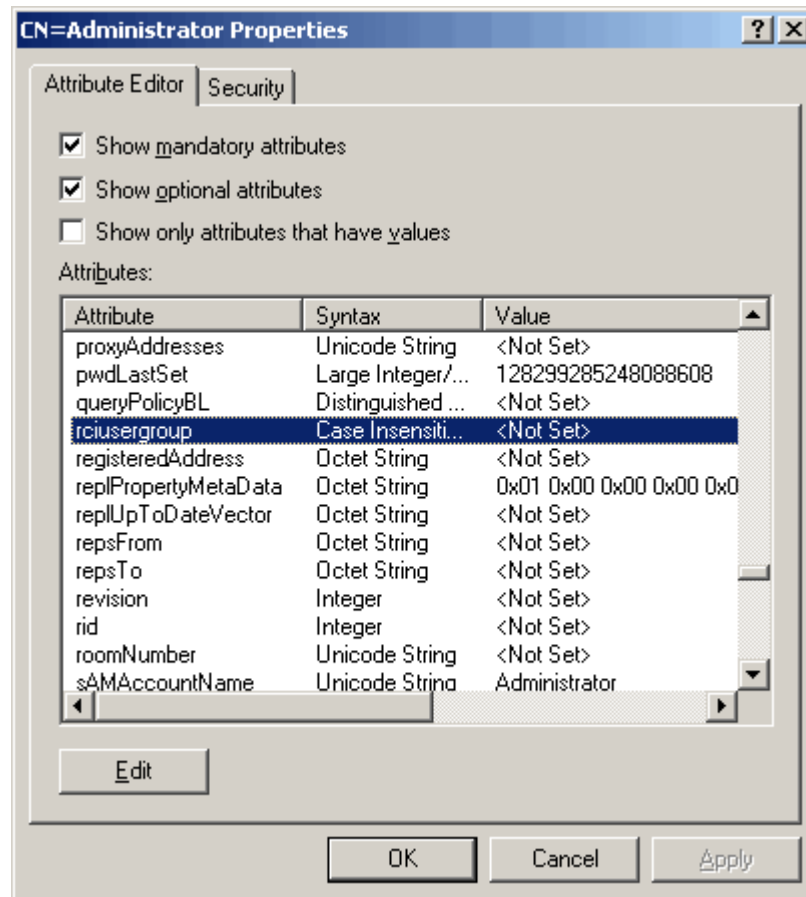
6. In the left pane of the window, select the CN=Users folder.



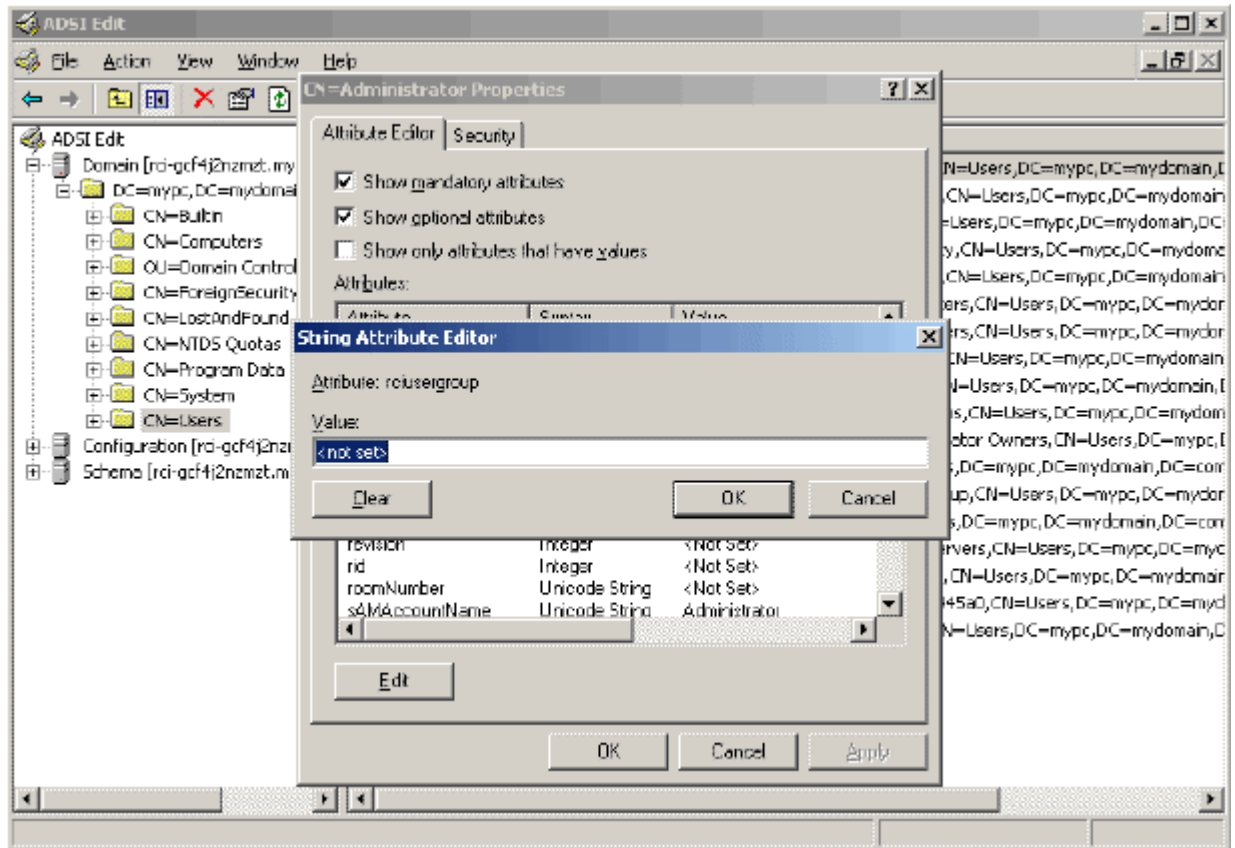
7. Locate the user name whose properties you want to adjust in the right pane. Right-click on the user name and select Properties.
8. Click on the Attribute Editor tab if it is not already open.

Editing rcusergroup Attributes for User Members

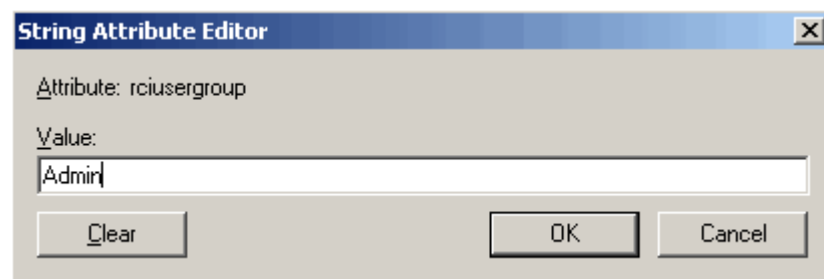
9. Choose rcusergroup from the Attributes list.



10. Click Edit. The String Attribute Editor dialog opens:



11. Type the user group (created in Dominion Dominion KX II) in the Edit Attribute field.



12. Click OK.

Appendix C Informational Notes

In This Chapter

Overview

Non-US Keyboards (on page 213)

Macintosh Keyboard (on page 216)

Mouse Pointer Synchronization (Fedora)

Resolving Fedora Core Focus

SUSE/VESA Video Modes

CIMs

Virtual Media

CC-SG

In This Chapter

Overview.....	212
Non-US Keyboards.....	213
Macintosh Keyboard	216
Special Sun Key Combinations	217
Mouse Pointer Synchronization (Fedora).....	217
Resolving Fedora Core Focus.....	218
SUSE/VESA Video Modes	218
CIMs	219
Virtual Media	219
CC-SG	220

Overview

This chapter includes important notes on Dominion KX II usage. Future updates will be documented and available online through the Help - User Guide link in the Dominion KX II Remote Console interface.

Non-US Keyboards

French Keyboard

Caret Symbol (Linux Clients only)

The Virtual KVM Client and the Multi-Platform Client (MPC) do not process the key combination of Alt Gr + 9 as the caret symbol (^) when using French keyboards with Linux clients.

➤ *To obtain the caret symbol:*

From a French keyboard, press the ^ key (to the right of the P key), then immediately press the space bar.

Alternatively, create a macro consisting of the following commands:

1. Press Right Alt
2. Press 9.
3. Release 9.
4. Release Right Alt.

Note: These procedures do not apply to the circumflex accent (above vowels). In all cases, the ^ key (to the right of the P key) works on French keyboards to create the circumflex accent when used in combination with another character.

Accent Symbol (Windows XP Clients only)

From the Virtual KVM Client and the Multi-Platform Client, the key combination of Alt Gr + 7 results in the accented character displaying twice when using French keyboards with Windows XP clients.

Note: This does not occur with Linux clients.

Numeric Keypad

From the Virtual KVM Client and the Multi-Platform Client, the numeric keypad symbols display as follows when using a French keyboard:

Numeric Keypad Symbol	Displays As
/	;
.	;

Tilde Symbol

From the Virtual KVM Client and the Multi-Platform Client, the key combination of Alt Gr + 2 does not produce the tilde (~) symbol when using a French keyboard.

➤ *To obtain the tilde symbol:*

Create a macro consisting of the following commands:

- Press Right Alt
- Press 2
- Release 2
- Release Right Alt

Caret Symbol (Linux Clients only)

The Virtual KVM Client and the Multi-Platform Client (MPC) do not process the key combination of Alt Gr + 9 as the caret symbol (^) when using French keyboards with Linux clients.

➤ *To obtain the caret symbol:*

From a French keyboard, press the ^ key (to the right of the P key), then immediately press the space bar.

Alternatively, create a macro consisting of the following commands:

1. Press Right Alt
2. Press 9.
3. Release 9.
4. Release Right Alt.

Note: These procedures do not apply to the circumflex accent (above vowels). In all cases, the ^ key (to the right of the P key) works on French keyboards to create the circumflex accent when used in combination with another character.

Accent Symbol (Windows XP Clients only)

From the Virtual KVM Client and the Multi-Platform Client, the key combination of Alt Gr + 7 results in the accented character displaying twice when using French keyboards with Windows XP clients.

Note: This does not occur with Linux clients.

Numeric Keypad

From the Virtual KVM Client and the Multi-Platform Client, the numeric keypad symbols display as follows when using a French keyboard:

Numeric Keypad Symbol	Displays As
/	;
.	;

Tilde Symbol

From the Virtual KVM Client and the Multi-Platform Client, the key combination of Alt Gr + 2 does not produce the tilde (~) symbol when using a French keyboard.

➤ *To obtain the tilde symbol:*

Create a macro consisting of the following commands:

- Press Right Alt
- Press 2
- Release 2
- Release Right Alt

Java Runtime Environment (JRE)

Because of a limitation in the Java Runtime Environment (JRE), Fedora, Linux, and Solaris clients receive an invalid response from Alt Gr on UK English and US International language keyboards. Fedora, Linux, and Solaris do not pick up events for the Alt Gr key combination for Java 1.4.2 or 1.5. Java 1.6 appears to improve on this, although the keyPressed and keyReleased events for Alt Gr still identify it as an “unknown key code”.

Also, a key pressed in combination with Alt Gr (such as on the UK keyboard Alt Gr-4), which is the Euro symbol), will only generate a keyTyped followed by a keyReleased event for that value, without a keyPressed event. Java 1.6 improves upon this by filling in the keyPressed event as well.

Keyboard Language Preference (Fedora Linux Clients)

There are several methods that can be used to set the keyboard language preference on Fedora Linux clients. The following method must be used in order for the keys to be mapped correctly from the Virtual KVM Client and the Multi-Platform Client (MPC).

➤ *To set the keyboard language:*

1. From the toolbar, select System > Preferences > Keyboard.
2. Open the Layouts tab.
3. Add or select the appropriate language.
4. Click Close.

Note: Other methods will not necessarily yield correct results.

Macintosh Keyboard

When a Macintosh is used as the client, the following keys on the Mac keyboard are not captured by the Java Runtime Environment (JRE):

- F9
- F10
- F11
- F14
- F15
- Volume Up
- Volume Down
- Mute
- Eject

As a result, the Virtual KVM Client and the Multi-Platform Client (MPC) are unable to process these keys from a Mac client's keyboard.

Special Sun Key Combinations

The following key combinations for Sun Microsystems server's special keys operate on the local port:

Sun Key	Local Port Key Combination
Again	Ctrl+ ALT +F2
Props	Ctrl + ALT +F3
Undo	Ctrl + ALT +F4
Stop A	Break a
Front	CTRL + ALT + F5
Copy	CTRL + ALT + F6
Open	CTRL + ALT + F7
Find	CTRL + ALT + F9
Cut	CTRL + ALT + F10
Paste	CTRL + ALT + F8
Mute	CTRL + ALT + F12
Compose	CTRL+ ALT + KPAD *
Vol +	CTRL + ALT + KPAD +
Vol -	CTRL + ALT + KPAD -
Stop	No key combination
Power	No key combination

Mouse Pointer Synchronization (Fedora)

When connected in dual mouse mode to a target server running Fedora 7, the target and local mouse pointers may lose synchronization after some time.

➤ *To re-synchronize the mouse cursors:*

Use the Synchronize Mouse option from the Virtual KVM Client.

Resolving Fedora Core Focus

The following table summarizes the Dominion KX II mouse modes, and whether or not these modes remain synchronized when accessing KVM target servers running Fedora:

Mouse Mode	Fedora Core 5	Fedora Core 6
Absolute Mouse Synchronization	No	No
Intelligent Mouse Mode	No	Yes
Standard Mouse Mode	Yes	No

Resolving Fedora Core Focus

Using the Multi-Platform Client (MPC), occasionally there is an inability to log into a Dominion KX II device or to access KVM target servers (Windows, SUSE, etc.). In addition, the Ctrl+Alt+M key combination may not bring up the Keyboard Shortcut menu. This situation occurs with the following client configuration: Fedora Core 6 and Firefox 1.5 or 2.0.

Through testing, it has been determined that installation of libXp resolves window focusing issues with Fedora Core 6. Raritan has tested with libXp-1.0.0.8.i386.rpm; this resolved all of the keyboard focus and popup-menu problems.

Note: libXp is also required for the SeaMonkey (formerly Mozilla) browser to work with the Java plugin.

SUSE/VESA Video Modes

The SuSE X.org configuration tool SaX2 generates video modes using modeline entries in the X.org configuration file. These video modes do not correspond exactly with VESA video mode timing (even when a VESA monitor is selected). Dominion KX II, on the other hand, relies on exact VESA mode timing for proper synchronization. This disparity can result in black borders, missing sections of the picture, and noise.

➤ *To configure the SUSE video display:*

1. The generated configuration file /etc/X11/xorg.conf includes a "Monitor" section with an option named UseModes. For example: UseModes "Modes[0]"
2. Either comment out this line (using #) or delete it completely.
3. Restart the X server.

With this change, the internal video mode timing from the X server will be used and will correspond exactly with the VESA video mode timing, resulting in the proper video display on the Dominion KX II.

CIMs

Windows 3-Button Mouse on Linux Targets

When using a 3-button mouse on a Windows client connecting to a Linux target, the left mouse button may get mapped to the center button of the Windows client 3-button mouse.

Virtual Media

Dell Optiplex and Dimension Computers

From certain Dell Optiplex and Dimension computers, it may not be possible to boot a target server from a redirected drive/ISO image, or to access the target server BIOS when a virtual media session is active (unless the Use Full Speed for Virtual Media CIM option is enabled from the Port page).

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

Virtual Media not Refreshed after Files Added

After a virtual media drive has been mounted, if you add a file(s) to that drive, those files may not be immediately visible on the target server. Disconnect and then reconnect the virtual media connection.

Target BIOS Boot Time with Virtual Media

The BIOS for certain targets may take longer to boot if media is mounted virtually at the target.

➤ *To shorten the boot time:*

1. Close the Virtual KVM Client to completely release the virtual media drives.
2. Restart the target.

CC-SG

Virtual KVM Client Version not Known from CC-SG Proxy Mode

When the Virtual KVM Client is launched from CommandCenter Secure Gateway (CC-SG) in proxy mode, the Virtual KVM Client version is unknown. In the About Raritan Virtual KVM Client dialog, the version is displayed as "Version Unknown".

Proxy Mode and MPC

If you are using Dominion KX II in a CC-SG configuration, do not use the CC-SG proxy mode if you are planning to use the Multi-Platform Client (MPC) or the Raritan Serial Client (RSC).

Appendix D FAQs

In This Chapter

General Questions (Shared).....	222
Remote Access.....	224
Universal Virtual Media	226
Ethernet and IP Networking	227
Servers.....	231
Installation	233
Local Port.....	235
Power Control	237
Scalability.....	238
Computer Interface Modules (CIMs).....	239
Security.....	240
Manageability.....	242
Miscellaneous.....	243
Troubleshooting.....	244

General Questions (Shared)

Question	Answer
What is Dominion KX II?	<p>Dominion KX II is a second generation digital KVM (Keyboard, Video Mouse) switch that enables IT administrators to access and control 8, 16, 32, or 64* servers over the network with BIOS-level functionality. Dominion KX II is completely hardware and OS-independent; users can troubleshoot and reconfigure servers even when servers are down.</p> <p>At the rack, Dominion KX II provides the same functionality, convenience, space savings, and cost savings as traditional analog KVM switches. However, Dominion KX II also integrates the industry's highest-performing KVM-over-IP technology, allowing multiple administrators to access server KVM consoles from any networked workstation.</p>
How does Dominion KX II differ from remote control software?	<p>When using Dominion KX II remotely, at first glance, the interface may seem similar to remote control software such as pcAnywhere, Windows Terminal Services / Remote Desktop, VNC, etc. However, because Dominion KX II is not a software but a hardware solution, it's much more powerful:</p> <p>OS- and hardware-independent - Dominion KX II can be used to manage servers running many popular operating systems, including Intel, Sun, PowerPC running Windows, Linux, Solaris, etc.</p> <p>State-independent / Agentless - Dominion KX II does not require the managed server OS to be up and running, nor does it require any special software to be installed on the managed server.</p> <p>Out-of-Band - Even if the managed server's own network connection is unavailable, it can still be managed through Dominion KX II.</p> <p>BIOS-level access - Even if the server is hung at boot up, requires booting to safe mode, or requires system BIOS parameters to be altered, Dominion KX II still works flawlessly to enable these configurations to be made.</p>
How do the new features of the Dominion KX II compare to the KX I?	<p>Dominion KX II has many new and exciting features, including virtual media, dual power, dual gigabit Ethernet, common Web-based user interfaces, next generation local port, etc.</p>

Question	Answer
How do I migrate from the Dominion KX I to Dominion KX II?	In general, customers can continue to use their existing switches for many years. As their data centers expand, customers can purchase and use the new Dominion KX II models. Raritan's centralized management appliance, CommandCenter Secure Gateway, and the Multi-Platform Client (MPC) both support KX I and Dominion KX II switches seamlessly.
Will my existing KX I CIMs work with the Dominion KX II switch?	Yes, existing KX I CIMs will work with the Dominion KX II switch. In addition, select Paragon CIMs will work with the Dominion KX II. This provides an easy migration to Dominion KX II from Paragon I customers who wish to switch to KVM-over-IP.
Can the Dominion KX II be rack mounted?	Yes. The Dominion KX II ships standard with 19" rack mount brackets. It can also be reverse rack mounted so the server ports face forward.
How large is the Dominion KX II?	Dominion KX II is only 1U high (except KX2-464, which is 2U), fits in a standard 19" rack mount, and is only 11.4" (29 cm) deep.

Remote Access

Question	Answer
How many users can remotely access servers on each Dominion KX II?	Dominion KX II models offer remote connections for up to eight users per channel for simultaneous access and control of a unique target server. For one-channel devices like the DKX2-116, up to eight remote users can access and control a single target server. For two-channel devices, like the DKX2-216, up to eight users can access and control the server on channel one and up to another eight users on channel two. For four-channel devices, up to eight users per channel, for a total of 32 (8 x 4) users, can access and control four servers in a similar fashion.
Can two people look at the same server at the same time?	Yes, actually up to eight people can access and control any single server at the same time.
Can two people access the same server, one remotely and one from the local port?	Yes, the local port is completely independent of the remote "ports." The local port can access the same server using the PC-Share feature.
In order to access Dominion KX II from a client, what hardware, software or network configuration is required?	<p>Because Dominion KX II is completely Web-accessible, it doesn't require installation of proprietary software on clients used for access.</p> <p>Dominion KX II can be accessed through major Web browsers including: Internet Explorer, Mozilla and Firefox. Dominion KX II can now be accessed on Windows, Linux, Sun Solaris and Macintosh desktops, via Raritan's Java-based Multi-Platform Client (MPC) and the new Virtual KVM Client.</p> <p>Dominion KX II administrators can also perform remote management (set passwords and security, rename servers, change IP address, etc.) using a convenient browser-based interface.</p>

Question	Answer												
What is the file size of the applet that is used to access Dominion KX II? How long does it take to retrieve?	<p>The Virtual KVM Client applet used to access Dominion KX II is approximately 500KB in size. The following chart describes the time required to retrieve Dominion KX II's applet at different network speeds:</p> <table><tr><td>100Mbps</td><td>Theoretical 100Mbit network speed</td><td>0.05 second s</td></tr><tr><td>60Mbps</td><td>Likely practical 100Mbit network speed</td><td>0.08 second s</td></tr><tr><td>10Mbps</td><td>Theoretical 10Mbit network speed</td><td>.4 second s</td></tr><tr><td>6Mbps</td><td>Likely practical 10Mbit network speed</td><td>.8 second s</td></tr></table>	100Mbps	Theoretical 100Mbit network speed	0.05 second s	60Mbps	Likely practical 100Mbit network speed	0.08 second s	10Mbps	Theoretical 10Mbit network speed	.4 second s	6Mbps	Likely practical 10Mbit network speed	.8 second s
100Mbps	Theoretical 100Mbit network speed	0.05 second s											
60Mbps	Likely practical 100Mbit network speed	0.08 second s											
10Mbps	Theoretical 10Mbit network speed	.4 second s											
6Mbps	Likely practical 10Mbit network speed	.8 second s											
How do I access servers connected to Dominion KX II if the network ever becomes unavailable?	Dominion KX II's local ports always allow access to servers from the rack, regardless of the network condition.												
Do you have a non-Windows client?	Yes. Both the Virtual KVM Client and the Multi-Platform Client (MPC), allow non-Windows users to connect to KVM target servers through the Dominion KX I and Dominion KX II switches. MPC can be run via Web browsers and standalone. Please refer to the <i>Virtual KVM Client</i> (on page 65) and the MPC/RRC User Guide for more information.												
Sometimes during a Virtual KVM Client session, the Alt key appears to get stuck. What should I do?	<p>This usually occurs in situations when the Alt key is held and not released. For instance, continuing to press the Alt key while pressing the space bar might cause the focus to change from the target server to the client PC.</p> <p>The local operating system then interprets this key combination and consequently triggers the action for this key combination in the active window (the client PC).</p>												

Universal Virtual Media

Question	Answer
What Dominion KX II models support virtual media?	All Dominion KX II models support virtual media. It is available standalone and through CommandCenter Secure Gateway, a centralized management appliance.
What types of virtual media does the Dominion KX II support?	Dominion KX II supports the following types of media: internal and USB-connected CD/DVD drives, USB mass storage devices, PC hard drives, and remote drives.
What is required for virtual media?	The new D2CIM-VUSB CIM is required for virtual media. It supports virtual media sessions to KVM target servers supporting the USB 2.0 interface. Available in economical 32 and 64 quantity CIM packages, this new CIM supports Absolute Mouse Synchronization as well as remote firmware update.
Is virtual media secure?	Yes. Virtual media sessions are secured using 128-bit AES or RC4 encryption.

Ethernet and IP Networking

Question	Answer
Does the Dominion KX II offer dual gigabit Ethernet ports to provide redundant failover, or load balancing?	Yes. Dominion KX II features dual gigabit Ethernet ports to provide redundant failover capabilities. Should the primary Ethernet port (or the switch/router to which it is connected) fail, Dominion KX II will failover to the secondary network port with the same IP address - ensuring that server operations are not disrupted. Note that automatic failover must be enabled by the administrator.

Question	Answer												
How much bandwidth does Dominion KX II require?	<p>Dominion KX II offers next generation KVM-over-IP technology - the very best video compression available. Raritan has received numerous technical awards confirming its high video quality transmissions and the low bandwidth utilization.</p> <p>Raritan pioneered the KVM-over-IP functionality that allows users to tailor their video parameters to conserve network bandwidth. With that in mind, the following data refers to Dominion KX II at its default video settings - again, these settings can be tailored to a specific environment. They can be increased to provide even higher quality video (color depth), or decreased to optimize for low-speed connections.</p> <p>As a general rule, a conservative estimate for bandwidth utilization (at Dominion KX II's default settings) is approximately 0.5Mbit/second per active KVM user (connected to and using a server), with very occasional spikes up to 2Mbit/second. This is a very conservative estimate because bandwidth utilization will typically be even lower.</p> <p>Bandwidth required by each video transmission depends on what task is being performed on the managed server. The more the screen changes, the more bandwidth is utilized. The table below summarizes some use cases and the required bandwidth utilization at Dominion KX II's default settings on a 10Mbit/s network:</p> <table border="1"> <tr> <td>Idle Windows Desktop</td><td>0 Mbps</td></tr> <tr> <td>Move Cursor Around Desktop</td><td>0.18Mbps</td></tr> <tr> <td>Move Static 400x600 Window/Dialog Box</td><td>0.35Mbps</td></tr> <tr> <td>Navigate Start Menu</td><td>0.49Mbps</td></tr> <tr> <td>Scroll an Entire Page of Text</td><td>1.23Mbps</td></tr> <tr> <td>Run 3D Maze Screensaver</td><td>1.55Mbps</td></tr> </table>	Idle Windows Desktop	0 Mbps	Move Cursor Around Desktop	0.18Mbps	Move Static 400x600 Window/Dialog Box	0.35Mbps	Navigate Start Menu	0.49Mbps	Scroll an Entire Page of Text	1.23Mbps	Run 3D Maze Screensaver	1.55Mbps
Idle Windows Desktop	0 Mbps												
Move Cursor Around Desktop	0.18Mbps												
Move Static 400x600 Window/Dialog Box	0.35Mbps												
Navigate Start Menu	0.49Mbps												
Scroll an Entire Page of Text	1.23Mbps												
Run 3D Maze Screensaver	1.55Mbps												
What is the slowest connection (lowest bandwidth) over which Dominion KX II can operate?	33Kbps or above is recommended for acceptable Dominion KX II performance.												

Question	Answer
What is the speed of Dominion KX II's Ethernet interfaces?	Dominion KX II supports Gigabit as well as 10/100 Ethernet. Dominion KX II supports two 10/100/1000 speed Ethernet interfaces, with configurable speed and duplex settings (either auto-detected or manually set).
Can I access Dominion KX II over a wireless connection?	Yes. Dominion KX II not only uses standard Ethernet, but also very conservative bandwidth with very high quality video. Thus, if a wireless client has network connectivity to a Dominion KX II, servers can be configured and managed at BIOS-level wirelessly.
Can Dominion KX II be used over the WAN (Internet), or just over the corporate LAN?	Whether via a fast corporate LAN or the less predictable WAN (Internet), Dominion KX II's KVM-over-IP technology can accommodate the connection.
Can I use Dominion KX II with a VPN?	Yes. Dominion KX II uses standard Internet Protocol (IP) technologies from Layer 1 through Layer 4. Traffic can be easily tunneled through standard VPNs.
How many TCP ports must be open on my firewall in order to enable network access to Dominion KX II? Are these ports configurable?	Only one. Dominion KX II protects network security by only requiring access to a single TCP port to operate. This port is completely configurable for additional security. Note that, of course, to use Dominion KX II's optional Web browser capability, the standard HTTPS port 443 must also be open.
Does Dominion KX II require an external authentication server to operate?	No. Dominion KX II is a completely self-sufficient. After assigning an IP address to a Dominion KX II, it is ready to use - with Web browser and authentication capabilities completely built-in. If an external authentication server (such as LDAP, Active Directory, RADIUS, etc.) is used, Dominion KX II allows this as well, and will even failover to its own internal authentication should the external authentication server become unavailable. In this way, Dominion KX II's design philosophy is optimized to provide ease of installation, complete independence from any external server, and maximum flexibility.
Can Dominion KX II be used with CITRIX?	Dominion KX II may work with remote access products like CITRIX if configured appropriately, but Raritan cannot guarantee it will work with acceptable performance. Products like CITRIX utilize video redirection technologies similar in concept to digital KVM switches so that two KVM-over-IP technologies are being used simultaneously.

Question	Answer
Can the Dominion KX II use DHCP?	DHCP addressing can be used, however, Raritan recommends fixed addressing since the Dominion KX II is an infrastructure device and can be accessed and administered more effectively with a fixed IP address.
I'm having problems connecting to the Dominion KX II over my IP network. What could be the problem?	<p>The Dominion KX II relies on your LAN/WAN network. Some possible problems include:</p> <p>Ethernet auto negotiation. On some networks, 10/100 auto negotiation does not work properly and the Dominion KX II unit must be set to 100MB/full duplex or the appropriate choice for its network.</p> <p>Duplicate IP Address. If the IP Address of the Dominion KX II is the same as another device, network connectivity may be inconsistent.</p> <p>Port 5000 conflicts. If another device is using port 5000, the Dominion KX II default port must be changed (or the other device must be changed).</p> <p>When changing the IP Address of a Dominion KX II, or swapping in a new Dominion KX II, sufficient time must be allowed for its IP and MAC addresses to be known throughout the Layer 2 and Layer 3 networks.</p>

Servers

Question	Answer
Does Dominion KX II depend on a Windows server to operate?	<p>Absolutely not. Because users depend on the KVM infrastructure to always be available in any scenario whatsoever (as they will likely need to use the KVM infrastructure to fix problems), Dominion KX II is designed to be completely independent from any external server.</p> <p>For example, should the data center come under attack from a malicious Windows worm or virus, administrators will need to use the KVM solution to resolve the situation. Therefore, it is imperative that the KVM solution, in turn, must not rely on these same Windows servers (or any server, for that matter) to be operational in order for the KVM solution to function.</p> <p>To this end, Dominion KX II is completely independent. Even if a user chooses to configure the Dominion KX II to authenticate against an Active Directory server - if that Active Directory server becomes unavailable, Dominion KX II's own authentication will be activated and fully functional.</p>
Do I need to install a Web server such as Microsoft Internet Information Services (IIS) in order to use Dominion KX II's Web browser capability?	No. Dominion KX II is a completely self-sufficient appliance. After assigning an IP address to Dominion KX II, it's ready to use - with Web browser and authentication capabilities completely built-in.
What software do I have to install in order to access Dominion KX II from a particular workstation?	None. Dominion KX II can be accessed completely via a Web browser. A Java-based client is now available for non-Windows users.
What should I do to prepare a server for connection to Dominion KX II?	Simply set the mouse parameters in order to provide users with the best mouse synchronization during remote connections, as well as turning off the power management features that effect screen display. However, if the new D2CIM-VUSB adapter is used (supporting Absolute Mouse Synchronization™), then manually setting the mouse parameters isn't necessary.

Servers

Question	Answer
What comes in the Dominion KX II box?	The following is included: (a) Dominion KX II unit; (b) Quick Setup Guide; (c) standard 19" rack mount brackets; (d) User manual CD-ROM; (e) Network cable; (f) Crossover cable; (g) Localized AC Line Cord; (h) Warranty certificate and other documentation.

Installation

Question	Answer
Besides the unit itself, what do I need to order from Raritan to install Dominion KX II?	Each server that connects to Dominion KX II requires a Dominion or Paragon Computer Interface Module (CIM), an adapter that connects directly to the keyboard, video, and mouse ports of the server.
What kind of Cat5 cabling should be used in my installation?	Dominion KX II can use any standard UTP (unshielded twisted pair) cabling, whether Cat5, Cat5e, or Cat6. Often in our manuals and marketing literature, Raritan will simply say "Cat5" cabling for short. In actuality, any brand UTP cable will suffice for Dominion KX II.
What types of servers can be connected to Dominion KX II?	Dominion KX II is completely vendor independent. Any server with standard-compliant keyboard, video, and mouse ports can be connected.
How do I connect servers to Dominion KX II?	Servers that connect to the Dominion KX II require a Dominion or Paragon CIM, which connects directly to the keyboard, video, and mouse ports of the server. Then, connect each CIM to Dominion KX II using standard UTP (twisted pair) cable such as Cat5, Cat5e, or Cat6.
How far can my servers be from Dominion KX II?	In general servers can be up to 150 feet (45 m) away from Dominion KX II depending on the type of server. (Please refer to the Raritan Web site or <i>Target Server Connection Distance</i> (see "Target Server Connection Distance and Video Resolution" on page 200) for more information.) For the new D2CIM-VUSB CIM that supports virtual media and Absolute Mouse Synchronization, a 100 (30 m) foot range is recommended.
Some operating systems lock up when I disconnect a keyboard or mouse during operation. What prevents servers connected to Dominion KX II from locking up when I switch away from them?	Each Dominion computer interface module (DCIM) dongle acts as a virtual keyboard and mouse to the server to which it is connected. This technology is called KME (keyboard/mouse emulation). Raritan's KME technology is data center grade, battle-tested, and far more reliable than that found in lower-end KVM switches: it incorporates more than 15 years of experience and has been deployed to millions of servers worldwide.
Are there any agents that must be installed on servers connected to Dominion KX II?	Servers connected to Dominion KX II do not require any software agents to be installed, because Dominion KX II connects directly via hardware to servers' keyboard, video, and mouse ports.

Installation

Question	Answer
How many servers can be connected to each Dominion KX II unit?	Dominion KX II models range from 8, 16, or 32 server ports in a 1U chassis to 64 server ports in a 2U chassis. This is the industry's highest digital KVM switch port density.
What happens if I disconnect a server from Dominion KX II and reconnect it to another Dominion KX II unit, or connect it to a different port on the same Dominion KX II unit?	Dominion KX II will automatically update the server port names when servers are moved from port to port. Furthermore, this automatic update does not just affect the local access port, but propagates to all remote clients and the optional CommandCenter Secure Gateway management appliance.
How do I connect a serially controlled (RS-232) device to Dominion KX II, such as a Cisco router/switch or a headless Sun server?	<p>If there are only a few serially-controlled devices, they may be connected to a Dominion KX II using Raritan's new P2CIM-SER serial converter.</p> <p>However, if there are four or more serially-controlled devices, we recommend the use of Raritan's Dominion KX II line of secure console servers. For multiple serial devices, Dominion KX II offers more serial functionality at a better price point than Dominion KX II. This SX is easy to use, configure and manage, and can be completely integrated with a Dominion Series deployment. In particular, many UNIX and networking administrators appreciate the ability to directly SSH to a Dominion KX II unit.</p>

Local Port

Question	Answer
Can I access my servers directly from the rack?	Yes. At the rack, Dominion KX II functions just like a traditional KVM switch - allowing control of up to 64 servers using a single keyboard, monitor, and mouse.
When I am using the local port, do I prevent other users from accessing servers remotely?	No. The Dominion KX II local port has a completely independent access path to the servers. This means a user can access servers locally at the rack - without compromising the number of users that access the rack remotely at the same time.
Can I use a USB keyboard or mouse at the local port?	Yes. Dominion KX II offers both PS/2 and USB keyboard and mouse ports on the local port. Note that the USB ports are USB v1.1, and support keyboards and mice only - not USB devices such as scanners or printers.
Is there an On-Screen Display (OSD) for local, at-the-rack access?	Yes, but Dominion KX II's at-the-rack access goes way beyond conventional OSDs. Featuring the industry's first browser-based interface for at-the-rack access, Dominion KX II's local port uses the same interface for local and remote access. Moreover, most administrative functions are available at-the-rack.
How do I select between servers while using the local port?	The local port displays the connected servers using the same user interface as the remote client. Connect to a server with a simple click of the mouse.
How do I ensure that only authorized users can access servers from the local port?	<p>Users attempting to use the local port must pass the same level of authentication as those accessing remotely. This means that:</p> <p>If the Dominion KX II is configured to interact with an external RADIUS, LDAP or Active Directory server, users attempting to access the local port will authenticate against the same server.</p> <p>If the external authentication servers are unavailable, Dominion KX II fails-over to its own internal authentication database.</p> <p>Dominion KX II has its own standalone authentication, enabling instant, out-of-the-box installation.</p>

Local Port

Question	Answer
If I use the local port to change the name of a connected server, does this change propagate to remote access clients as well? Does it propagate to the optional CommandCenter appliance?	Yes. The local port presentation is identical and completely in sync with remote access clients, as well as Raritan's optional CommandCenter Secure Gateway management appliance. To be clear, if the name of a server via the Dominion KX II on-screen display is changed, this updates all remote clients and external management servers in real-time.
If I use Dominion KX II's remote administration tools to change the name of a connected server, does that change propagate to the local port OSD as well?	Yes. If the name of a server is changed remotely, or via Raritan's optional CommandCenter Secure Gateway management appliance, this update immediately affects Dominion KX II's on-screen display.
Sometimes I see "shadows" on the local port user interface. Why does that occur?	This shadow/ghosting effect may occur with LCD monitors that have been on for long periods. The LCD properties and the electrical/static charge can produce these effects when the screen is on for a long time.

Power Control

Question	Answer
Does Dominion KX II have a dual power option?	All Dominion KX II models come equipped with dual AC inputs and power supplies with automatic fail-over. Should one of the power inputs or power supplies fail, then the Dominion KX II will automatically switch to the other.
Does the power supply used by Dominion KX II automatically detect voltage settings?	Yes. Dominion KX II's power supply can be used in AC voltage ranges from 100-240 volts, at 50-60 Hz.
If a power supply or input fails, will I be notified?	The Dominion KX II front panel LED will notify the user of a power failure. An entry will also be sent to the Audit Log and displayed on the Dominion KX II Remote Client User Interface. If configured by the administrator, then SNMP or Syslog events will be generated.
What type of power control capabilities does Dominion KX II offer?	Raritan's Remote Power Control power strips can be connected to the Dominion KX II to provide power control of the KVM target servers. After a simple one-time configuration step, just right click on the server name to power on, off, or recycle a hung server. Note that a hard reboot provides the physical equivalent of unplugging the server from the AC power line, and reinserting the plug.
Does Dominion KX II support servers with multiple power supplies? What if each power supply is connected to a different power strip?	Yes. Dominion KX II can be easily configured to support multiple power supplies connected to multiple power strips. Up to eight (8) power strips can be connected to a Dominion KX II device. Four power supplies can be connected per target server to multiple power strips.
Does remote power control require any special server configuration?	Some servers ship with default BIOS settings such that the server does not automatically restart after losing and regaining power. See the server user manual for more information.
What type of power strips does Dominion KX II support?	To take advantage of Dominion KX II's integrated power control user interface, and more importantly, integrated security, use Raritan's Remote Power Control (RPC) power strips. RPCs come in many outlet, connector, and amp variations. The D2CIM-PWR must be purchased to connect the RPC to the Dominion KX II.

Scalability

Question	Answer
How do I connect multiple Dominion KX II devices together into one solution?	<p>Multiple Dominion KX II units do not need to be physically connected together. Instead, each Dominion KX II unit connects to the network, and they automatically work together as a single solution if deployed with Raritan's optional CommandCenter Secure Gateway (CC-SG) management appliance. CC-SG acts as a single access point for remote access and management. CC-SG offers a significant set of convenient tools, such as consolidated configuration, consolidated firmware update, and a single authentication and authorization database.</p> <p>In addition, CC-SG enables sophisticated server sorting, permissions, and access. If deployment of Raritan's CC-SG management appliance isn't an option, multiple Dominion KX II units still interoperate and scale automatically: The Dominion KX II's remote user interface and the Multi-Platform Client will automatically discover Dominion KX II units. Non-discovered Dominion KX II units can be accessed via a user-created profile.</p>
Can I connect an existing analog KVM switch to Dominion KX II?	<p>Yes. Analog KVM switches can be connected to one of Dominion KX II's server ports. Simply use a PS/2 Computer Interface Module (CIM), and attach it to the user ports of the existing analog KVM switch. Please Note that analog KVM switches vary in their specifications and Raritan cannot guarantee the interoperability of any particular third-party analog KVM switch. Contact Raritan technical support for further information. Raritan's Paragon and Paragon II analog switches are IP-enabled by the IP-Reach family of remote access products.</p>

Computer Interface Modules (CIMs)

Question	Answer
Can I use Computer Interface Modules (CIMs) from Raritan's analog matrix KVM switch, Paragon, with Dominion KX II?	<p>Yes. Certain Paragon computer interface modules (CIMs) may work with Dominion KX II (please check the Raritan Dominion KX II release notes on the web site for the latest list of certified CIMs).</p> <p>However, because Paragon CIMs cost more than Dominion KX II CIMs (as they incorporate technology for video transmission of up to 1000 feet [300 meters]), it is not generally advisable to purchase Paragon CIMs for use with Dominion KX II. Also note that when connected to Dominion KX II, Paragon CIMs transmit video at a distance of up to 150 feet, the same as Dominion KX II CIMs - not at 1000 feet [300 meters], as they do when connected to Paragon.</p>
Can I use Dominion KX II Computer Interface Modules (CIMs) with Raritan's analog matrix KVM switch, Paragon?	<p>No. Dominion KX II computer interface modules (CIMs) transmit video at ranges of 50 to 150 feet (15 - 45 m) and thus do not work with Paragon, which requires CIMs that transmit video at a range of 1000 feet (300 meters). To ensure that all Raritan's customers experience the very best quality video available in the industry - a consistent Raritan characteristic - Dominion Series CIMs do not interoperate with Paragon.</p>

Security

Question	Answer
What kind of encryption does Dominion KX II use?	Dominion KX II uses industry-standard (and extremely secure) 128-bit RC4 or AES encryption, both in its SSL communications as well as its own data stream. Literally no data is transmitted between remote clients and Dominion KX II that is not completely secured by encryption.
Does Dominion KX II support AES encryption as recommended by the US Government's NIST and FIPS standards?	The Dominion KX II utilizes the Advanced Encryption Standard (AES) encryption for added security. AES is a US government approved cryptographic algorithm that is recommended by the National Institute of Standards and Technology (NIST) in the FIPS Standard 197.
Does Dominion KX II allow encryption of video data? Or does it only encrypt keyboard and mouse data?	Unlike competing solutions, which only encrypt keyboard and mouse data, Dominion KX II does not compromise security - it allows encryption of keyboard, mouse and video data.
How does Dominion KX II integrate with external authentication servers such as Active Directory, RADIUS, or LDAP?	Through a very simple configuration, Dominion KX II can be set to forward all authentication requests to an external server such as LDAP, Active Directory, or RADIUS. For each authenticated user, Dominion KX II receives from the authentication server the user group to which that user belongs. Dominion KX II then determines the user's access permissions depending on the user group to which he or she belongs.
How are usernames and passwords stored?	Should Dominion KX II's internal authentication capabilities be used, all sensitive information such as usernames and passwords are stored in an encrypted format. Literally no one, including Raritan technical support or Product Engineering departments, can retrieve those usernames and passwords.
Does Dominion KX II support strong password?	Yes. The Dominion KX II has administrator-configurable, strong password checking to ensure that user-created passwords meet corporate and/or government standards and are resistant to brute force hacking.

Question	Answer														
If the Dominion KX II Encryption Mode is set to Auto, what level of encryption is achieved?	<p>The encryption level that is auto-negotiated is dependent on the browser in use:</p> <table> <thead> <tr> <th data-bbox="586 453 808 485">Browser</th><th data-bbox="841 453 1040 485">Encryption Level</th></tr> </thead> <tbody> <tr> <td data-bbox="586 506 808 537">Internet Explorer 6</td><td data-bbox="841 506 889 537">RC4</td></tr> <tr> <td data-bbox="586 558 808 590">Internet Explorer 7</td><td data-bbox="841 558 938 590">AES-128</td></tr> <tr> <td data-bbox="586 611 808 642">Firefox 1.5</td><td data-bbox="841 611 889 642">RC4</td></tr> <tr> <td data-bbox="586 663 808 695">Firefox 2.0</td><td data-bbox="841 663 889 695">RC4</td></tr> <tr> <td data-bbox="586 716 808 747">Mozilla 1.7</td><td data-bbox="841 716 889 747">RC4</td></tr> <tr> <td data-bbox="586 768 808 800">Safari 2.0.4</td><td data-bbox="841 768 938 800">AES-128</td></tr> </tbody> </table>	Browser	Encryption Level	Internet Explorer 6	RC4	Internet Explorer 7	AES-128	Firefox 1.5	RC4	Firefox 2.0	RC4	Mozilla 1.7	RC4	Safari 2.0.4	AES-128
Browser	Encryption Level														
Internet Explorer 6	RC4														
Internet Explorer 7	AES-128														
Firefox 1.5	RC4														
Firefox 2.0	RC4														
Mozilla 1.7	RC4														
Safari 2.0.4	AES-128														

Manageability

Question	Answer
Can Dominion KX II be remotely managed and configured via Web browser?	<p>Yes. Dominion KX II can be completely configured remotely via Web browser. Note that this does require that the workstation have an appropriate Java Runtime Environment (JRE) version installed.</p> <p>Besides the initial setting of Dominion KX II's IP address, everything about the solution can be completely set up over the network. (In fact, using a crossover Ethernet cable and Dominion KX II's default IP address, you can even configure the initial settings via Web browser.)</p>
Can I backup and restore Dominion KX II's configuration?	<p>Yes. Dominion KX II's device and user configurations can be completely backed up for later restoration in the event of a catastrophe.</p> <p>Dominion KX II's backup and restore functionality can be used remotely over the network, or through a Web browser.</p>
What auditing or logging does Dominion KX II offer?	For complete accountability, Dominion KX II logs all major user events with a date and time stamp. For instance, reported events include (but are not limited to): user login, user logout, user access of a particular server, unsuccessful login, configuration changes, etc.
Can Dominion KX II integrate with Syslog?	Yes. In addition to Dominion KX II's own internal logging capabilities, Dominion KX II can send all logged events to a centralized Syslog server.
Can Dominion KX II integrate with SNMP?	Yes. In addition to Dominion KX II's own internal logging capabilities, Dominion KX II can send SNMP traps to SNMP management systems like HP Openview and Raritan's CC-NOC.
Can Dominion KX II's internal clock be synchronized with a timeserver?	Yes. Dominion KX II supports the industry-standard NTP protocol for synchronization with either a corporate timeserver, or with any public timeserver (assuming that outbound NTP requests are allowed through the corporate firewall).

Miscellaneous

Question	Answer
What is Dominion KX II's default IP address?	192.168.0.192
What is Dominion KX II's default username and password?	The Dominion KX II's default username and password are admin/raritan [all lower case]. However, for the highest level of security, the Dominion KX II forces the administrator to change the Dominion KX II default administrative username and password when the unit is first booted up.
I changed and subsequently forgot Dominion KX II's administrative password; can you retrieve it for me?	Dominion KX II contains a hardware reset button that can be used to factory reset the device, which will reset the administrative password on the device.

Troubleshooting

Question	Answer
I am logged into the Dominion KX II using Firefox, and I opened another Firefox browser. I am automatically logged into the same Dominion KX II with the second Firefox browser. Is this right?	Yes, this is correct behavior and is the direct result of how browsers and cookies function.
I am logged into the Dominion KX II using Firefox and I attempt to log into another Dominion KX II using another Firefox browser session from the same client. I am logged out of both Dominion KX IIs; is this correct behavior?	Yes, to access two different Dominion KX II devices, either close the first session, or use another client PC.
When I'm running a KVM session using Firefox as my browser, and certain dialogs are opened in the Virtual KVM Client (e.g., Connection Properties, Video Settings), it seems to block the Firefox browser (even other Firefox sessions). What can I do?	This is normal behavior; with Firefox, all sessions are associated. Once you close the Virtual KVM Client dialog, Firefox will no longer be blocked.

Index

1

- 1. AC Power • 29

2

- 2. Network Ports • 30

3

- 3. Local Access Port (local PC) • 30

4

- 4. Target Server Ports • 31, 35

A

- About Raritan Virtual KVM Client • 86
- Absolute • 16, 83
- Accent Symbol (Windows XP Clients only) • 212
- Accessing a Target Server • 187
- Accessing KVM Target Servers • 58, 186
- Add a New User Group (Shared) • 104
- Add New Favorite • 52, 57
- Add New User • 100, 101, 102, 156
- Add New User Group • 103, 106
- Adding Attributes to the Class • 203
- Apple Macintosh Settings • 27
- Assigning an IP Address • 34
- Associate KVM Target Servers to Outlets (Port Page) • 36, 143, 148
- Audit Log • 163, 183, 192
- Authentication Settings • 114
- Authentication vs. Authorization • 37, 114, 191
- Auto-sense Video Settings • 77
- Available Resolutions • 185

B

- Backup and Restore • 42, 166

C

- Calibrate Color • 78
- Caret Symbol (Linux Clients only) • 212

- CC-SG • 218
- CD-ROM/DVD-ROM/ISO Images • 91, 95, 97
- Change Password • 113
- Change the Keyboard Layout Code (Sun Targets) • 28, 126
- Changing the Default Password • 32
- Checking Your Browser for AES Encryption • 157, 159
- CIM Upgrade • 168
- CIMs • 217
- Computer Interface Modules (CIMs) • 196, 237
- Conditions when Read-Write is not Available • 93, 94
- Connect the Power Strip • 144
- Connecting to a KVM Target Server • 60
- Connecting to the Dominion KX II • 40
- Connecting to Virtual Media • 93
- Connection Info • 72
- Connection Menu • 70
- Creating a Keyboard Macro • 74
- Creating a New Attribute • 202

D

- Date/Time Settings • 129
- Default IP Address • 10
- Dell OpTIPlex and Dimension Computers • 217
- Desktop Background • 16
- Device Diagnostics • 42, 179
- Device Information • 165
- Device Management • 122
- Device Management Menu • 122
- Diagnostics • 173
- Diagnostics Menu • 173
- Disconnecting KVM Target Servers • 62
- Disconnecting Virtual Media • 91, 96
- Discover Devices - KX Subnet • 56
- Discover Devices - Local Subnet • 54
- Dominion KX II Console Layout • 47
- Dominion KX II Console Menu Tree • 48, 185
- Dominion KX II Console Navigation • 47
- Dominion KX II Local Console • 181, 182

Index

- Dominion KX II Devices • 41, 185
- Dominion KX II Local Console Interface • 185
- Dominion KX II Overview • 2
- Dominion KX II Remote Console
 - Dominion KX II Devices • 42

E

- Editing rcusergroup Attributes for User Members • 206
- Encryption & Share • 90, 153, 156, 183
- Environmental Requirements • 194
- Ethernet and IP Networking • 225
- Event Management • 130
- Event Management - Destinations • 136
- Event Management - Settings • 131
- Exit • 72

F

- Factory Reset (Dominion KX II Local Console Only) • 41, 192
- FAQs • 219
- Favorites List • 52
- File Server Setup (File Server ISO Images Only) • 91, 97
- French Keyboard • 211
- From LDAP • 201
- From Microsoft Active Directory • 201

G

- General Questions (Shared) • 220
- Getting Started • 10
- Group-based IP ACL (Access Control List) • 106, 108, 109, 112, 128, 159
- Groups • 38

H

- Hardware • 4
- Help Menu • 86
- Hotkeys • 61, 62, 187

I

- IBM AIX 5.3 Settings • 26
- Implementing LDAP Remote Authentication • 115, 117

- Implementing RADIUS Remote Authentication • 115, 119
- Informational Notes • 44, 210
- Installation • 231
- Installation and Configuration • 14, 69
- Intelligent • 16, 83
- Introduction • 1
- IP Access Control • 106, 108, 110, 128, 159

J

- Java Runtime Environment (JRE) • 45, 213

K

- Keyboard Language Preference (Fedora Linux Clients) • 214
- Keyboard Macros • 73
- Keyboard Menu • 73

L

- LAN Interface Settings • 30, 124, 127
- Language Support • 44
- Launching the Dominion KX II • 45
- Linux Settings (Red Hat 4) • 21
- Linux Settings (Red Hat 9) • 19
- Local Drives • 91, 93
- Local Port • 233
- Local Port Administration • 188
- Local Port Settings (Dominion KX II Local Console Only) • 41, 187, 189
- Logging Out • 48
- Login Information • 10
- Login Limitations • 152, 153

M

- Macintosh Keyboard • 210, 214
- Maintenance • 162
- Maintenance Features (Local/Remote Console) • 162
- Maintenance Menu • 162
- Make Linux Settings Permanent • 23
- Make UNIX Settings Permanent • 27
- Manage Favorites Menu • 51
- Manageability • 240
- Managing Favorites • 42, 50
- Menu Tree • 66

- Miscellaneous • 241
- Modify Existing User • 100, 102
- Modify Existing User Group • 103, 112
- Modifying a Keyboard Macro • 76
- Mouse Menu • 68, 81
- Mouse Pointer Synchronization • 68
- Mouse Pointer Synchronization (Fedora) • 215
- Mouse Settings • 16
- Mouse Synchronization Tips • 68
- Multi-Platform Client (MPC)
 - KX I and Dominion KX II Devices • 43

N

- Name the Power Strip (Port Page for Power Strips) • 143, 146
- Naming Target Servers • 35
- Network Basic Settings • 124, 125
- Network Interface Page • 174
- Network Miscellaneous Settings • 55, 124, 126
- Network Settings • 28, 34, 35, 123, 160, 197
- Network Speed Settings • 127, 199
- Network Statistics Page • 174
- Non-US Keyboards • 210, 211
- Note for D2CIM-VUSB CIM Usage (Shared) • 27, 148, 150
- Note on Microsoft Active Directory • 37
- Note to CC-SG Users • 36
- Numeric Keypad • 213

O

- Opening a KVM Session • 91, 92
- Operating System Mouse and Video Settings • 16
- Options • 66, 84
- Organization of Information • 8
- Overview • 14, 65, 88, 210

P

- Package Contents • 7
- Physical Connections • 183, 185
- Physical Specifications • 194
- Ping Host Page • 177
- Port Access Page • 59
- Port Action Menu • 60, 186, 187
- Port Configuration Page • 142, 146, 148

- Power Control • 144, 235
- Power Controlling a Target Server • 62
- Power Cycle a Target Server • 62
- Power Off a Target Server • 63
- Power On a Target Server • 63
- Power Supply Setup Page • 30, 36, 140
- Prerequisites for Using Virtual Media • 90, 91
- Product Features • 4
- Product Photos • 3
- Properties Dialog • 70
- Proxy Mode and MPC • 218

R

- RADIUS Communication Exchange
 - Specifications • 120
- Raritan Remote Client (RRC)
 - Dominion KX II Devices Only • 44
- Reboot • 171
- Refresh Screen • 77
- Related Documentation • 9
- Relationship between Users and Groups • 39
- Remote Access • 222
- Remote Authentication • 36, 191
- Remote Connection • 196
- Removing a Keyboard Macro • 76
- Reset Button • 158, 183
- Resolving Fedora Core Focus • 216
- Returning to the Dominion KX II Local
 - Console Interface • 187
- Returning User Group Information • 201
- Returning User Group Information from
 - Active Directory Server • 117
- Returning User Group Information via
 - RADIUS • 120
- Running a Keyboard Macro • 76

S

- Scalability • 236
- Scaling • 85
- Security • 238
- Security and Authentication • 185
- Security Settings • 101, 151, 152
- Security Settings Menu • 151
- Send Ctrl+Alt+Delete • 73
- Server Display • 186

Index

- Servers • 229
- Set Permissions for Individual Group • 102, 113
- Setting Permissions • 108
- Setting Port Permissions • 90, 106, 108, 109, 112
- Setting the Registry to Permit Write Operations to the Schema • 202
- Simultaneous Users • 184
- Single Mouse Cursor • 82
- SNMP Agent Configuration • 131, 133, 137
- SNMP Configuration • 133
- SNMP Trap Configuration • 131, 133, 137
- Software • 5
- Special Sun Key Combinations • 215
- Specifications • 31, 194
- Specifying Power Supply Auto-detection • 36
- Standard • 16, 82
- Starting the Dominion KX II Local Console • 184
- Step 1
 - Configure KVM Target Servers • 15, 81
- Step 2 (Optional)
 - Configure Keyboard Language • 28
- Step 3
 - Configure Network Firewall Settings • 28
- Step 4
 - Connect the Equipment • 29
- Step 5
 - Dominion KX II Initial Configuration • 31
- Strong Passwords • 114, 152, 154
- Sun Solaris Settings • 23
- Supported Browsers • 11
- Supported Operating Systems (Clients) (Shared) • 10
- Supported Operating Systems and CIMs (Target Servers) • 11
- Supported Protocols • 37
- Supported Video Resolutions • 15
- SUSE Linux 10.1 Settings • 22
- SUSE/VESA Video Modes • 216
- Switching Between KVM Target Servers • 61
- Synchronize Mouse • 81
- Syslog Configuration • 135

T

- Target BIOS Boot Time with Virtual Media • 217
- Target Screen Resolution • 86
- Target Server Connection Distance and Video Resolution • 15, 68, 198, 231
- TCP and UDP Ports Used • 197
- Terminology • 5, 15
- Tilde Symbol • 213
- Toolbar • 67
- Tools Menu • 84
- Trace Route to Host Page • 178
- Troubleshooting • 242

U

- Universal Virtual Media • 224
- Updating the LDAP Schema • 117, 201
- Updating the Schema Cache • 205
- Upgrade History • 42, 170
- User Blocking • 152, 155
- User Group List • 103
- User Guide • 7
- User Interfaces • 40
- User List • 100
- User Management • 99, 185
- User Management Menu • 99
- Users • 38
- Users, Groups, and Access Permissions • 37
- Using Virtual Media • 91

V

- Valid Special Characters • 32, 34, 36, 113, 146, 149
- Video Menu • 77
- Video Settings • 78
- View Menu • 85
- View Toolbar • 85
- Virtual KVM Client • 60, 62, 64, 92, 223
- Virtual KVM Client Version not Known from CC-SG Proxy Mode • 218
- Virtual Media • 3, 42, 83, 87, 217
- Virtual Media not Refreshed after Files Added • 217

W

Windows 2000 Settings • 18

Windows 3-Button Mouse on Linux Targets •
217

Windows Vista • 18

Windows XP / Windows 2003 Settings • 17



➤ *U.S./Canada/Latin America*

Monday - Friday
8 a.m. - 8 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

➤ *China*

Beijing, China

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai, China

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou, China

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

➤ *India*

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

➤ *Korea*

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +82-2-5578730

➤ *Taiwan*

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: tech.rap@raritan.com

➤ *Europe*

Europe

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom

Monday - Friday
8:30 a.m. to 5 p.m. GMT+1 CET
Phone +44-20-7614-77-00

France

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0

➤ *Japan*

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5994
Email: support.japan@raritan.com

➤ *Melbourne, Australia*

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

